Hybrid Mesh Network Security

09 September 2026

SCALABLE PLATFORMS

R82

Administration Guide

CHECK POINT™

Check Point Copyright Notice

© 2024 - 2026 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

Important Information

Latest Software

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

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R82

For more about this release, see the R82 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
09 September 2026	Updated: ■ *"Upgrading Maestro Environment to R82" on page 52* ■ *"Upgrading Scalable Chassis to R82 - Zero Downtime (MVC)" on page 272*
22 July 2026	Added limitations section: ■ *"Introduction" on page 27* ■ *"Getting Started with ElasticXL Cluster" on page 35*
19 July 2026	Updated: ■ *"Working with the Distribution Mode" on page 554*
19 July 2026	Updated: ■ *"Upgrading Maestro Environment to R82" on page 52*
29 April 2026	Updated: ■ *"asg_policy" on page 797*
16 April 2026	Updated: ■ *"General Workflow in Maestro" on page 99*
09 March 2026	Updated: ■ *"Upgrading Maestro Environment to R82" on page 52* - updated "Important Notes for Maestro Orchestrators" Removed: ■ "Working with the GARP Chunk Mechanism" - obsolete
02 February 2026	Updated: ■ *"ElasticXL Important Notes" on page 33*
13 January 2026	Updated: ■ *"Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC)" on page 505* ■ *"g_clusterXL_admin" on page 896*

Date	Description
08 January 2026	Updated: ■ *"Upgrading Maestro Environment to R82" on page 52*
04 January 2026	Updated: ■ *"System Monitoring on Security Groups" on page 640*
09 December 2025	Updated: ■ *"insights" on page 903*
20 July 2025	Added: ■ *"Selecting Active Site in VSLS" on page 576* Updated: ■ *"Upgrading Maestro Environment to R82" on page 52* ■ *"Upgrading Scalable Chassis to R82 - Zero Downtime (MVC)" on page 272* ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 518* ■ *"Installing a Hotfix on Dual Chassis" on page 335* ■ *"Installing a Hotfix on a Single Chassis" on page 318* ■ *"Uninstalling a Hotfix from Dual Chassis" on page 343* ■ *"Uninstalling a Hotfix from a Single Chassis" on page 328* ■ *"lightshot" on page 900*
29 June 2025	Updated: ■ *"Upgrading Hardware Components on Scalable Chassis" on page 433*
28 June 2025	Updated: ■ *"Working with the Distribution Mode" on page 554* ■ *"SNMP for Security Group Members" on page 670*

Date	Description
28 Apr 2025	Added: ■ *"Configuring Link State Propagation (LSP) on a Maestro Orchestrator" on page 258* ■ *"reboot" on page 917* Updated: ■ *"Configuring Link State Propagation (LSP) on Scalable Chassis" on page 368* ■ *"SNMP for Security Groups" on page 647* ■ *"Configuring Bond Interface on the Management Ports of a Maestro Security Group" on page 179* ■ *"add maestro" on page 999* ■ *"set maestro" on page 1027* ■ *"show maestro" on page 1034* ■ *"delete maestro" on page 1012*
25 March 2025	Updated: ■ *"Maestro Auto-Scaling" on page 217*
17 March 2025	Updated: ■ *"lightshot" on page 900*
10 March 2025	Updated: ■ *"set maestro" on page 1027* - added warnings for the command "`set maestro port <Name>`" Removed: ■ The CLI command "`asg_session_control`" - it is not supported anymore
09 March 2025	Updated: ■ *"Getting Started with ElasticXL Cluster" on page 35*

Date	Description
08 March 2025	Updated: ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 518* Updated the notes to apply so this procedure applies to ElasticXL Cluster as well ■ *"Getting Started with ElasticXL Cluster" on page 35* Added steps to get the MAC Address for the license in the VSNext mode ■ *"Connecting to a Specific Security Group Member in Maestro" on page 206*
18 February 2025	Updated: ■ *"Maestro Fastforward" on page 227*
16 December 2024	Updated: ■ *"Maestro Fastforward" on page 227*
21 November 2024	Updated: ■ *"lightshot" on page 900*
19 November 2024	Updated: ■ *"asg_blade_config" on page 709* - ElasticXL does not support the "`asg_blade_config set_sync_start_ip`" command
14 November 2024	Updated: ■ *"Installing and Uninstalling a Hotfix on Maestro Orchestrators" on page 82* - removed the unnecessary best practice to take a Gaia Snapshot on the Orchestrator

Date	Description
22 October 2024	Added: ■ *"Upgrading Scalable Chassis to R82 - Zero Downtime (MVC)" on page 272* ■ *"Rolling Back a Failed Upgrade of a Maestro Orchestrator from R82" on page 79* ■ *"Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC)" on page 505* ■ *"asg monitor (on Maestro Orchestrator)" on page 1001* ■ *"member" on page 909* ■ *"ccutil" on page 1073* Updated: ■ *"Working with ElasticXL Cluster" on page 30* ■ *"Upgrading Maestro Environment to R82" on page 52* ■ *"Installing a Hotfix on Dual Chassis" on page 335* ■ *"Uninstalling a Hotfix from Dual Chassis" on page 343* ■ *"Upgrading the CMM Firmware on N+1 Scalable Chassis" on page 434* ■ *"Upgrading the CMM Firmware on N+N Scalable Chassis - CMM700" on page 442* ■ *"Upgrading the CMM Firmware on N+N Scalable Chassis - CMM500" on page 466* ■ *"Replacing SSM160 with SSM440 on Scalable Chassis" on page 482* ■ *"cluster-cli" on page 863* ■ *"cluster_site_admin" on page 874* ■ *"set cluster members-admin-state" on page 933* ■ *"set cluster members-reboot" on page 935* ■ *"orch_stat" on page 1017* Removed: ■ Deprecated commands (drop_monitor, asg_collect_vsx_logs, asg_affinity_enhance`TP-16517`)
21 October 2024	First release of this document

Table of Contents

Introduction ... *27*
What is a Scalable Platform? ... *27*
Limitations ... *27*
How a Scalable Platform Works? ... *27*
Benefits of Scalable Platform Network Security ... *28*
Single Management Object (SMO) ... *29*
Working with ElasticXL Cluster ... *30*
ElasticXL Cluster Overview ... *30*
ElasticXL Network Diagram ... *31*
ElasticXL Important Notes ... *33*
Getting Started with ElasticXL Cluster ... *35*
Limitations ... *35*
ElasticXL Configuration ... *35*
Part 1 - Installation of Appliances ... *35*
Part 2 - Gaia First Time Configuration Wizard ... *35*
Part 3 - Configuration of ElasticXL Cluster ... *38*
Part 4 - Configuration in SmartConsole ... *38*
Part 5 - Adding other ElasticXL Cluster Members ... *38*
Part 6 - Installing licenses on ElasticXL Cluster Members ... *43*
Removing a Cluster Member from ElasticXL Cluster ... *46*
Moving an ElasticXL Cluster Member between ElasticXL Sites ... *46*
Installing and Uninstalling a Hotfix on ElasticXL Cluster ... *46*
Troubleshooting Log Files ... *47*
FAQ ... *47*
Working with Quantum Maestro ... *48*
Maestro Overview ... *48*
Maestro Security Groups ... *49*

Introduction to Maestro ... 50
Important Links ... 50
Getting Started with Maestro ... 51
Upgrading Maestro to R82 ... 52
Upgrading Maestro Environment to R82 ... 52
Rolling Back a Failed Upgrade of a Maestro Orchestrator from R82 ... 79
Installing and Uninstalling a Hotfix on Maestro Orchestrators ... 82
Installing a Hotfix Package on Orchestrators ... 82
Uninstalling a Hotfix Package on Orchestrators ... 84
Deleting a Hotfix Package on Orchestrators ... 84
Authentication between Maestro Orchestrators ... 85
Introduction ... 85
Authentication statuses in Gaia Portal and CLI ... 86
Configuring new authentication between Maestro Orchestrators ... 87
Forcing existing authentication between Maestro Orchestrators ... 91
Revoking existing authentication between Maestro Orchestrators ... 93
Blocking authentication with a Maestro Orchestrator ... 96
Troubleshooting ... 97
Configuring Security Groups in Maestro ... 98
General Workflow in Maestro ... 99
Step 1 - Configuration Procedure in Maestro ... 104
Workflow for Configuring Security Groups in Maestro ... 105
Summary of Configuration Options in Maestro ... 107
Configuring Security Groups in Maestro in Gaia Portal ... 111
Configuring Security Groups in Maestro in Gaia Clish ... 124
Step 2 - Configuring Gaia Settings of a Security Group in Maestro ... 159
Step 3 - Configuration of a Maestro Security Group in SmartConsole ... 161
Step 4 - License Installation in Maestro ... 170
Adding Licenses ... 170
Removing Licenses from a Specific Security Group Member ... 172

Step 5 - Special Configuration Scenarios in Maestro ... 173
Configuring Weights for Security Group Members in Maestro ... 174
Introduction ... 174
Limitations ... 174
Calculating the Security Group Member Weight ... 175
Configuring the Security Group Member Weights ... 176
Monitoring the Security Group Member Weights ... 177
Best Practices ... 178
Configuring Bond Interface on the Management Ports of a Maestro Security Group ... 179
Configuring Bond Interface on Uplink Ports of a Maestro Security Group ... 183
Configuring VLAN Interfaces on top of a Bond Interface on Uplink Ports of a Maestro Security Group ... 186
Procedure ... 186
Example ... 191
Configuring VLAN Interfaces on Uplink Ports a Maestro Security Group ... 195
Introduction ... 195
Viewing VLAN Interfaces on Uplink Ports in Gaia Portal ... 196
Viewing VLAN Interfaces on Uplink Ports in Gaia Clish ... 197
Configuring More Than 4000 VLAN Interfaces on Orchestrators ... 198
Shared Uplink Ports on a Maestro Security Group ... 200
Prerequisites ... 200
Known Limitations ... 200
Requirements for LACP bond that contains shared interfaces ... 200
Configuration ... 201
Configuring an LACP bond that contains shared uplink interfaces ... 201
LACP bond verification ... 203
Removing subordinate interfaces from LACP bonds ... 203
Removing an LACP bond that contains shared uplink interfaces from a Security Group ... 205
Managing Security Groups in Maestro ... 206

Connecting to a Specific Security Group Member in Maestro ... 206
Configuring a Unique IP Address per Site (UIPS) in Maestro Dual Site ... 208
Managing Orchestrator Ports ... 211
Managing Orchestrator Ports in Gaia Portal ... 211
Managing Orchestrator Ports in Gaia Clish ... 213
Monitoring Orchestrator Ports in Gaia Clish ... 213
Monitoring Orchestrator Ports in the Expert mode ... 213
System Monitoring in Maestro ... 214
SNMP for Maestro Orchestrators ... 214
Prerequisites ... 214
Supported SNMP OIDs for Maestro Orchestrators ... 215
Supported SNMP Trap OIDs for Maestro Orchestrators ... 216
System Optimization in Maestro ... 217
Maestro Auto-Scaling ... 217
Introduction to Maestro Auto-Scaling ... 217
Prerequisites for Maestro Auto-Scaling ... 217
Limitations of Maestro Auto-Scaling ... 217
Terms in Maestro Auto-Scaling ... 218
Configuration of Maestro Auto-Scaling ... 218
Monitoring of Maestro Auto-Scaling on Orchestrator ... 222
Troubleshooting of Maestro Auto-Scaling ... 225
Maestro Fastforward ... 227
Introduction to Maestro Fastforward ... 227
How Maestro Fastforward Works ... 228
FAQ for Maestro Fastforward ... 228
Topologies for Maestro Fastforward ... 229
Configuration of Maestro Fastforward ... 230
Monitoring Maestro Fastforward ... 236
Maestro Fastforward Considerations for Administrators ... 238
Routing Mechanism in Maestro Fastforward ... 239

Policy Mechanism in Maestro Fastforward ... 239
Special Considerations for Maestro Fastforward ... 243
Known Limitations of Maestro Fastforward ... 246
Troubleshooting of Maestro Fastforward ... 250
Configuring a Dedicated Logging Port in Maestro ... 253
Configuring Security Group High Availability in Maestro ... 255
Setting Security Group Weights (High Availability Factors) ... 255
Setting the Quality Grade Differential ... 256
Configuring Identity Based Access Control and Threat Prevention in Maestro ... 257
Configuring Link State Propagation (LSP) on a Maestro Orchestrator ... 258
Introduction to LSP ... 258
Configuration ... 258
Troubleshooting in Maestro ... 263
Installing the Gaia Operating System on a Maestro Orchestrator ... 263
Reset an Orchestrator to Factory Defaults ... 264
Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device ... 265
Log and Configuration Files in Maestro ... 266
Replacing a Maestro Orchestrator ... 269
Working with Quantum Scalable Chassis ... **270**
Introduction to Scalable Chassis ... 272
Licensing ... 272
Upgrading Scalable Chassis to R82 - Zero Downtime (MVC) ... 272
Initial Software Installation and Configuration on Scalable Chassis ... 294
Step 1: Installing the SGM Image on Scalable Chassis ... 294
Installing the SGM Image from a Removable Media ... 294
Upgrading the SGM220 BIOS Firmware ... 297
Step 2: Connecting Scalable Chassis to the Network ... 299
Step 3: Initial Software Configuration on Scalable Chassis ... 300
Step 4: Configuration of Scalable Chassis in SmartConsole ... 301
Configuring a Security Gateway Object for Scalable Chassis in SmartConsole ... 302

Configuring a Security Gateway Object ... 302
Confirming the Policy Installation ... 305
Confirming the Security Gateway Software Configuration ... 306
Configuring a Legacy VSX Gateway Object for Scalable Chassis in SmartConsole ... 307
Before creating the Legacy VSX Gateway ... 307
The VSX Gateway Wizard ... 308
Wizard Step 1: Defining VSX Gateway General Properties ... 309
Wizard Step 2: Selecting Virtual Systems Creation Templates ... 309
Wizard Step 3: Establishing SIC Trust ... 310
Wizard Step 4: Defining Physical Interfaces ... 310
Virtual Network Device Configuration ... 311
Wizard Step 5: VSX Gateway Management ... 312
Wizard Step 7: Completing the VSX Wizard ... 313
Confirming the VSX Gateway Software Configuration ... 314
Step 5: Licensing and Registration on Scalable Chassis ... 315
Installing and Uninstalling a Hotfix on SGMs on Scalable Chassis ... 317
Installing a Hotfix on a Single Chassis ... 318
Important Notes ... 318
Procedure ... 320
Uninstalling a Hotfix from a Single Chassis ... 328
Important Notes ... 328
Procedure ... 329
Installing a Hotfix on Dual Chassis ... 335
Important Notes ... 335
Procedure ... 336
Uninstalling a Hotfix from Dual Chassis ... 343
Important Notes ... 343
Procedure ... 344
Managing Security Groups on Scalable Chassis ... 350
Security Group on Scalable Chassis ... 350

Viewing SGMs in a Security Group on Scalable Chassis ... 350
Adding SGMs to a Security Group on Scalable Chassis ... 351
Deleting SGMs from a Security Group on Scalable Chassis ... 353
Connecting to a Specific Security Group Member on Scalable Chassis ... 354
Changing the Gaia Management Interface on Scalable Chassis ... 355
Configuring the SGM Range on Scalable Chassis ... 357
System Optimization on Scalable Chassis ... 358
Configuring Hyper-Threading on Scalable Chassis ... 358
Configuring a Dedicated Logging Port on Scalable Chassis ... 359
Working with Jumbo Frames on Scalable Chassis ... 361
Configuring Support for Jumbo Frames in a Security Group in the Gateway mode ... 361
Configuring Support for Jumbo Frames in a Security Group in the Traditional VSX mode ... 363
Confirming Jumbo Frames Configuration on SSM440 (asg_chassis_ctrl) ... 364
Confirming Jumbo Frames Configuration on SGMs and SGM Interfaces (asg_jumbo_conf show) ... 365
Working with Rx and Tx Ring Parameters on Scalable Chassis ... 366
Viewing the Current Configuration ... 366
Configuring the Rx (Receive) Ring Parameter ... 366
Configuring the Tx (Rransmit) Ring Parameter ... 366
Configuring the Rx (Receive) and Tx (Transmit) Ring Parameters ... 367
Configuring Link State Propagation (LSP) on Scalable Chassis ... 368
Background ... 368
Configuring LSP Port Groups on Scalable Chassis ... 368
Adding an LSP Port Group on Scalable Chassis ... 369
Deleting an LSP Port Group on Scalable Chassis ... 370
Dual Chassis in Active/Standby High Availability Mode ... 371
How Dual Chassis Active/Standby Mode Works ... 371
Background ... 371
Configuring Dual Chassis Active/Standby Mode ... 372
Synchronizing Dual Chassis on a Wide Area Network ... 373

Configuring Scalable Chassis High Availability ... 374
Configuring Chassis Weights (Chassis High Availability Factors) ... 374
Configuring the Chassis ID ... 376
Configuring the Quality Grade Differential ... 377
Configuring the Failover Freeze Interval ... 378
Configuring the Chassis Priority ... 379
Advanced Dual Chassis Features ... 380
The Interface Link Preemption Mechanism in Dual Chassis ... 380
The Sync Lost Mechanism in Dual Chassis ... 382
Managing the Connection Synchronization in Dual Chassis ... 384
Working with SyncXL in Dual Chassis ... 385
Setting the Administratively DOWN State on First Join in Dual Chassis ... 387
Configuring a Unique IP Address per Site (UIPS) in Dual Chassis ... 389
Monitoring Link State of Management Interfaces in Dual Chassis ... 392
Dual Chassis in Bridge Mode ... 396
Bridge Mode Topologies ... 396
BPDU ... 397
Configuring Bridge Interfaces in a Security Group in the Gateway Mode ... 397
Configuring Bridge Interfaces in a Security Group in the Traditional VSX Mode ... 398
Configuring Virtual Systems in Bridge Mode to Forward Non-IP Protocols ... 399
Hardware Monitoring and Control on Scalable Chassis ... 400
Advanced Hardware Configuration on Scalable Chassis ... 401
Configuring Port Speed on Scalable Chassis ... 402
SSM Port Speed on Scalable Chassis ... 402
Configuring the Speed of SSM Ports 1-7 on Scalable Chassis ... 403
Configuring the QSFP Port Mode for SSM Ports on Scalable Chassis ... 404
Viewing the SSM Port Speed on Scalable Chassis ... 406
Configuring the Management Port Speed on Scalable Chassis ... 409
Chassis Management Modules (CMMs) on Scalable Chassis ... 410
Background ... 410

Connecting to the Active CMM ... 410
Connecting to the Standby CMM ... 411
Collecting the CMM Diagnostic Information (clia fruinfo) ... 411
Changing the CMM Administrator Password ... 413
Changing the Chassis Configuration ... 414
CMM Commands ... 414
Security Switch Modules (SSMs) on Scalable Chassis ... 415
SSM CLI ... 415
Viewing the SSM Logs ... 418
Changing the Load Distribution on SGM Groups ... 419
Changing the SSM Administrator Password ... 420
Mapping of SSM Port IDs to SGM Port IDs ... 422
Checking the Connectivity from the SGMs to the SSMs ... 424
Adding or Removing SSMs After Initial Setup ... 424
Security Gateway Modules (SGMs) on Scalable Chassis ... 429
Background ... 429
Identifying SGMs in the Chassis (asg_detection) ... 429
Slot IDs for SGMs and SSMs on Scalable Chassis ... 431
Upgrading Hardware Components on Scalable Chassis ... 433
Upgrading the CMM Firmware on N+1 Scalable Chassis ... 434
Part 1 - Upgrading the CMM Firmware on the Standby Chassis ... 434
Part 2 - Failing Over from Active Chassis to Standby Chassis ... 438
Part 3 - Upgrading the CMM Firmware on the former Active Chassis ... 438
Upgrading the CMM Firmware on N+N Scalable Chassis - CMM700 ... 442
Upgrading the CMM Firmware on CMM700 - With Physical Access to Standby Chassis ... 442
Part 1 - Upgrading the CMM Firmware on the Standby Chassis ... 442
Part 2 - Failing Over from Active Chassis to Standby Chassis ... 447
Part 3 - Upgrading the CMM Firmware on the former Active Chassis ... 447
Upgrading the CMM Firmware on CMM700 - No Physical Access to Standby Chassis ... 453

Part 1 - Upgrading the CMM Firmware on the Standby Chassis ... 453
Part 2 - Failing Over from Active Chassis to Standby Chassis ... 459
Part 3 - Upgrading the CMM Firmware on the former Active Chassis ... 459
Upgrading the CMM Firmware on N+N Scalable Chassis - CMM500 ... 466
Part 1 - Upgrading the CMM Firmware on the Standby Chassis ... 466
Part 2 - Failing Over from Active Chassis to the Standby Chassis ... 473
Part 3 - Upgrading the CMM Firmware on the former Active Chassis ... 473
Upgrading SSM Firmware on Scalable Chassis ... 481
Replacing SSM160 with SSM440 on Scalable Chassis ... 482
Replacing SSM160 with SSM440 on a Single Chassis ... 482
Replacing SSM160 with SSM440 on Dual Chassis ... 484
Part 1 - Replacing SSM160 with SSM440 on the Chassis ... 484
Part 2 - Failing Over from the Active Chassis to the Standby Chassis ... 486
Part 3 - Replacing SSM160 with SSM440 on the former Active Chassis ... 486
Replacing Hardware Components on Scalable Chassis ... 490
Adding or Replacing an SGM on Scalable Chassis ... 490
Using Snapshot Image to Add a New or a Replacement SGM ... 490
Installing a New SGM Using a CD/DVD Device ... 499
Replacing the CMM on Scalable Chassis ... 500
Prerequisites ... 500
Replacing the CMM ... 500
Correcting an Incorrect Chassis Type ... 502
Troubleshooting on Scalable Chassis ... 503
Log Files on Scalable Chassis ... 503
Common Procedures for Scalable Platforms ... 504
Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC) ... 505
Rolling Back If Only Some of the Security Group Members Were Upgraded - Zero Downtime ... 505
Rolling Back the Whole Security Group - Zero Downtime ... 511
Installing and Uninstalling a Hotfix on Security Group Members ... 518

Important Notes ... 518
Installing a Hotfix Package on Security Group Members ... 519
Uninstalling a Hotfix Package on Security Group Members ... 528
Managing Security Groups ... 535
Single Management Object and Policies ... 535
Single Management Object ... 535
Installing and Uninstalling Policies ... 538
Working with Policies in CLI ... 538
Policy Management on Security Group Members ... 539
Synchronizing Policy and Configuration Between Security Group Members ... 540
Understanding the Configuration File List ... 541
Global Commands on Security Groups ... 543
Working with Global Commands ... 543
Gaia Global Commands ... 544
Check Point Global Commands ... 550
Backing Up and Restoring Gaia Configuration ... 553
Working with the Distribution Mode ... 554
Background ... 554
Automatic Distribution Configuration (Auto-Topology) ... 556
Manual Distribution Configuration (Manual-General) ... 559
Setting and Showing the Distribution Configuration (set distribution configuration) 560
Configuring the Interface Distribution Mode (set distribution interface) ... 562
Showing Distribution Status (show distribution status) ... 564
Running a Verification Test (show distribution verification) ... 568
Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode) ... 569
Setting the Administratively DOWN State on First Join ... 571
NAT and the Correction Layer in the Gateway Mode ... 573
NAT and the Correction Layer in the VSNext / Traditional VSX Mode ... 574
Selecting Active Site in VSLS ... 576
Overview of VSLS ... 576

Algorithm to Select an Active Site in VSLS ... 576
Deploying a Security Group in Monitor Mode ... 578
Introduction to Monitor Mode ... 578
Example Topology for Monitor Mode ... 579
Supported Software Blades in Monitor Mode ... 580
Limitations in Monitor Mode ... 582
Configuring a Security Group in the 'Gateway' mode in Monitor Mode ... 583
Configuring a Security Group in the 'Traditional VSX' mode in Monitor Mode ... 596
Configuring Specific Software Blades for Monitor Mode ... 608
Configuring the Threat Prevention Software Blades for Monitor Mode ... 609
Configuring the Application Control and URL Filtering Software Blades for Monitor Mode ... 611
Configuring the Data Loss Prevention Software Blade for Monitor Mode ... 612
Configuring the Security Group in Monitor Mode Behind a Proxy Server ... 614
Deploying a Security Group in Bridge Mode ... 615
Introduction to Bridge Mode ... 615
Example Topology for Bridge Mode ... 616
Supported Software Blades in Monitor Mode ... 617
Limitations in Bridge Mode ... 619
Configuring a Security Group in Bridge Mode ... 620
Accept, or Drop Ethernet Frames with Specific Protocols ... 630
Routing and Bridge Interfaces ... 632
IPv6 Neighbor Discovery ... 633
Managing Ethernet Protocols in Bridge Mode ... 634
System Optimization on Security Groups ... 636
Configuring Services to Synchronize After a Delay ... 636
Firewall Connections Table Size for Traditional VSX Gateway ... 639
System Monitoring on Security Groups ... 640
CPView ... 641
Overview of CPView ... 641

CPView User Interface ... 641
Using CPView ... 642
Working with SNMP ... 643
SNMP for Maestro Orchestrators ... 644
Prerequisites ... 644
Supported SNMP OIDs for Maestro Orchestrators ... 645
Supported SNMP Trap OIDs for Maestro Orchestrators ... 646
SNMP for Security Groups ... 647
Prerequisites ... 647
Supported SNMP OIDs for Security Groups ... 648
Supported SNMP Trap OIDs for Security Groups ... 655
SNMP Monitoring of Security Groups in the VSNext / Traditional VSX Mode ... 666
Common SNMP OIDs for Security Groups ... 667
SNMP for Security Group Members ... 670
Background ... 670
Limitations ... 671
Prerequisites ... 672
Enabling SNMP for Specific Security Group Members ... 673
Files ... 676
Monitoring Performance ... 677
Monitoring Traffic ... 678
Monitoring Interfaces ... 679
Monitoring VPN Tunnels ... 680
SmartConsole ... 680
SNMP ... 680
CLI Tools ... 680
Hardware Monitoring on Security Groups ... 681
Troubleshooting on Security Groups ... 682
Collecting System Information ... 682
General Diagnostic in Security Groups ... 683

Working with Command Line ... *686*
Syntax Legend for CLI Commands ... *687*
Command Completion in Gaia gClish ... *689*
Command History in Gaia gClish ... *691*
Moving and Editing in Gaia gClish ... *693*
Configuration Lock in Gaia gClish ... *695*
Summary of Gaia gClish Commands ... *697*
Common CLI Commands ... *699*
asg alert ... *699*
asg_arp ... *705*
asg_blade_config ... *709*
asg_blade_stats ... *712*
asg_br_verifier, asg_brs_verifier ... *720*
asg_clear_table ... *723*
asg_conns ... *725*
asg_cores_stats ... *727*
asg_cp2blades ... *730*
asg_dr_verifier ... *732*
asg_dst_route ... *735*
asg_dxl ... *738*
asg_excp_conf ... *744*
asg_gre ... *752*
asg_hd_space ... *753*
asg_ifconfig ... *757*
asg_igmp ... *766*
asg_ips_failover_behavior ... *771*
asg_license_verifier ... *773*
asg log ... *775*
asg_log_servers ... *780*
asg_lsp_util ... *783*

asg_mac_resolver ... 784
MAC Addresses and Bit Conventions ... 785
MAC Address Resolver ... 788
asg_mac_verifier, mac_verifier ... 789
asg monitor (on Security Groups) ... 792
asg_policy ... 797
asg_mroute ... 801
asg_pim neighbors ... 804
asg_pim ... 806
asg_process_verifier ... 809
asg_provision ... 810
asg_reboot ... 811
asg_route ... 813
add smo ... 824
asg stat ... 829
asg_swb_update_verifier ... 843
asg_tracert ... 851
asg_unique_mac_utility ... 852
asg_vsx_verify ... 855
clock_verifier ... 861
cluster-cli ... 863
cluster_site_admin ... 874
config_verify ... 876
core_dump_verifier ... 879
cpha_vsx_util monitor ... 881
delete cluster ... 883
delete smo ... 886
fw ctl get ... 888
fw ctl set ... 890
g_all, g_allc, g_alls ... 892

g_clusterXL_admin ... 896
hcp ... 899
lightshot ... 900
insights ... 903
member ... 909
Description ... 909
Syntax on ElasticXL Cluster ... 910
Syntax on Maestro Orchestrator ... 911
Syntax on Maestro Security Group ... 912
Syntax on Scalable Chassis ... 914
Related Commands ... 916
reboot ... 917
set cluster ... 920
set cluster alert_threshold ... 921
set cluster configuration high-availability ... 925
set cluster configuration image ... 930
set cluster configuration unique-ip ... 931
set cluster members-admin-state ... 933
set cluster members-reboot ... 935
set cluster sites-admin-state ... 937
set cluster site-id <Site ID> admin-state ... 939
set cluster site-id <Site ID> alert_threshold ... 941
set cluster site-id <Site ID> general ... 943
set cluster site-id <Site ID> module ... 944
set cluster site-id <Site ID> modules_amount ... 946
set cluster vsls ... 948
set distribution ... 950
set smo ... 954
show cluster ... 956
show cluster alert_threshold ... 957

show cluster configuration high-availability ... 960
show cluster configuration image ... 964
show cluster configuration unique-ip ... 965
show cluster info ... 967
show cluster site-id <ID> alert_threshold ... 975
show cluster site-id <Site ID> general ... 977
show cluster site-id <Site ID> module ... 978
show cluster site-id <Site ID> modules_amount ... 982
show cluster vsls ... 986
show distribution ... 988
show smo ... 990
tcpdump ... 992
update_conf_file ... 995
ver ... 998
CLI Commands for Maestro Orchestrator ... 999
add maestro ... 999
asg monitor (on Maestro Orchestrator) ... 1001
cplink ... 1003
delete maestro ... 1012
orch_info ... 1015
orch_stat ... 1017
orchd ... 1025
set maestro ... 1027
show maestro ... 1034
CLI Commands for Scalable Chassis ... 1041
asg_chassis_ctrl ... 1041
asg_hard_reboot ... 1045
asg_hard_shutdown ... 1047
asg_hard_start ... 1049
asg hw_monitor ... 1051

asg_jumbo_conf ... 1057
asg_serial_info ... 1062
asg_sgm_serial ... 1064
asg_traffic_stats ... 1066
asg_version ... 1068
ccutil ... 1073
Glossary ... ***1078***

Introduction

This Administration Guide describes the following Check Point products that are based on the Scalable Platform technology:

- ElasticXL Cluster - see *"Working with ElasticXL Cluster" on page 30*.
- Quantum Maestro - see *"Working with Quantum Maestro" on page 48*.
- Quantum Scalable Chassis - see *"Working with Quantum Scalable Chassis" on page 270*.

Note - For configuration of Software Blades, refer to the applicable Administration Guides in sk181127 - Check Point Quantum R82 Release.

What is a Scalable Platform?

Scalable Platform tightly integrates the compute, storage, security, and virtualization layers into a single solution. Scalable Platform design allows architecture to scale as needed to meet increased demand by provisioning additional resources on demand to existing systems. Scalable Platform environments offer full high availability, intelligent load balancing, and support for orchestration.

HyperScale network security solutions are designed to ensure the security of an organization's traffic and network environment while supporting extremely high availability and performance.

Limitations

- Adding or removing an unassigned interface from a Sync bond resets the flags. As a result, ElasticXL detection is disrupted, and ElasticXL drops the packet.

How a Scalable Platform Works?

Scalable Platform systems are designed to deliver the highest availability, resiliency, and security with easy scalability. The goal of Scalable Platform environments is to ensure that resources are always available to meet operational and business needs, and can grow on-demand without forklift upgrades or service disruption.

This is accomplished by networking computers horizontally, making it possible to rapidly spin systems up or down as needed. In front of these servers is a load balancer that directs requests to an available system. If a system is down or overloaded, other systems can help with the load, including the ability to spin up additional compute resources when needed.

A Scalable Platform system helps eliminate single points of failure or bottlenecks, which requires considering both networking and security functionality. A Scalable Platform system may integrate a high availability firewall with a load balancer to inspect all traffic at the firewall before routing it on to a server to fill the request. Resilient, redundant firewalls with integrated load balancing ensure that corporate IT infrastructure can scale and recover from issues without compromising security.

Benefits of Scalable Platform Network Security

Scalable Platform network security is a modern approach to ensuring the scalability and resiliency of the network security architecture protecting an organization's IT systems. Some of the top benefits of Scalable Platform architectures include the following:

- Dynamic Scalability with Ease:

  Scalability is one of the key functions of Scalable Platform architectures, enabling 10x – 50x scaling within a matter of minutes. This scaling is accomplished by spinning up additional load-balanced resources, enabling seamless expansion.

- Simplicity:

  Scalable Platform network security architectures are designed to treat an array of firewalls as a single unit. This makes it possible to add capacity or upgrade systems without the need to reconfigure the firewall cluster.

- Cloud-Level Resiliency:

  Cloud computing offers great resiliency and availability but is not suitable for all applications. Scalable Platform architectures can enable on-premises systems to achieve similar levels of resiliency without the security concerns of the public cloud.

- Cost Effectiveness:

  Scalable Platform data centers commonly use intelligent load balancing and multiple firewalls in a cluster to achieve full resiliency. Scalable Platform utilizes all of the compute resources in the cluster (vs. legacy 1+1 designs where half of all resources are in pure "standby" mode and not utilized). Scalable Platform provides maximum resiliency at a much lower cost of hardware, power/cooling, and real estate (rack space).

Single Management Object (SMO)

You manage a Scalable Platform as one Security Gateway or one Legacy VSX Gateway object in the Check Point security management GUI client, SmartConsole.

A single IP address for the Scalable Platform for management communication and policy installation simplifies the management.

All Scalable Platform Security Group Members automatically clone all software packages, settings, and security policies from the SMO.

Working with ElasticXL Cluster

Note - This chapter describes the unique procedures that apply only to an ElasticXL Cluster.
For additional procedures that apply to all Scalable Platforms, see the chapter *"Common Procedures for Scalable Platforms" on page 504*.

ElasticXL Cluster Overview

ElasticXL is a new clustering technology delivering simplified operations with a Single Management Object (SMO) and automatic sync of configuration and software between all cluster members.

ElasticXL Cluster provides a better administrator experience and performance than ClusterXL:

- Install and configure only the first Security Appliance (this is the SMO).

  Additional ElasticXL Cluster Members automatically clone the configuration and software packages from this SMO.
- The entire ElasticXL Cluster is represented by one Security Gateway object (SMO).
- Efficient scale architecture - ability to add and remove ElasticXL Cluster Members on-the-fly (the configuration and software packages are cloned automatically from the SMO).
- Global Gaia Portal and Global Gaia Clish to manage the entire ElasticXL Cluster.
- Dual Site support.
- Automatic configuration of the internal synchronization network.
- Support for Gaia RESTful API.

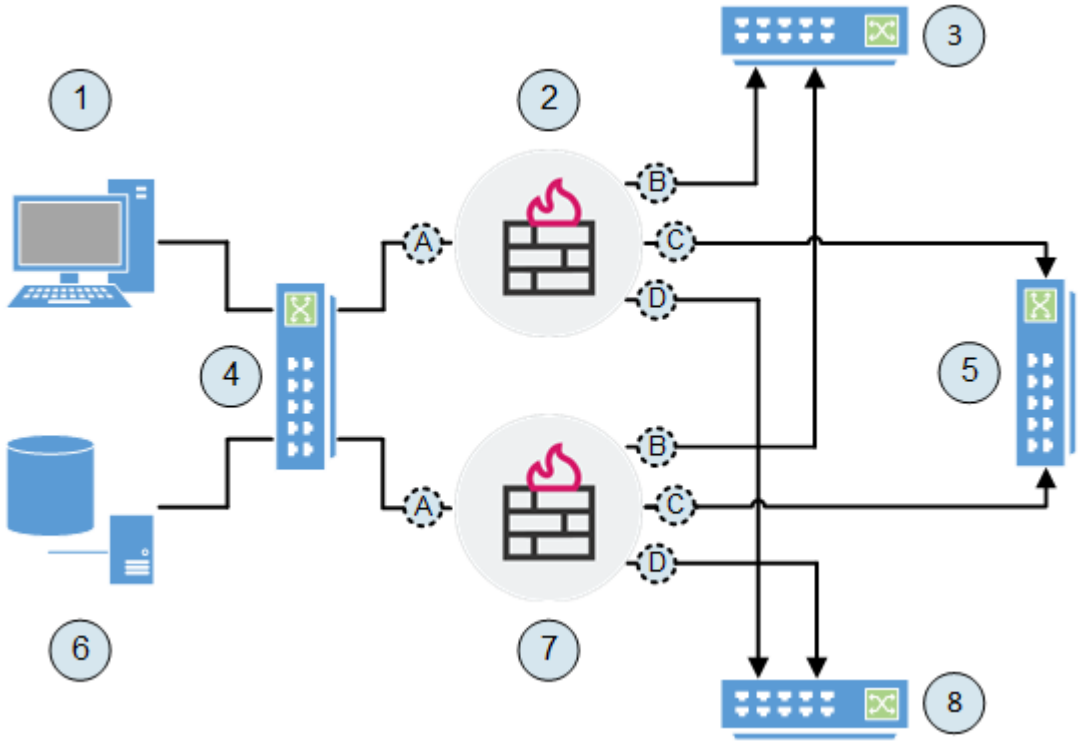
Note - To see the maximum numbers of supported items in ElasticXL, see the *R82 Release Notes* > Chapter "**Maximum Supported Items**".

ElasticXL Network Diagram

Below is a simplified network diagram for connecting Check Point appliances in the ElasticXL Cluster configuration.

This diagram shows only two Check Point appliances for simplicity.

This diagram shows four different switches only to explain the required connections.



Legend

Item	Description
1	SmartConsole client
2	First ElasticXL Cluster Member
3	External switch
4	Management switch
5	Synchronization switch
6	Security Management Server
7	Second ElasticXL Cluster Member
8	Internal switch

Legend (continued)

Item	Description
A	Management interface
B	External interface
C	Synchronization interface
D	Internal interface

ElasticXL Important Notes

- For the list of platforms that support ElasticXL, see the *R82 Release Notes*.
- For ElasticXL requirements, see sk183513.
- ElasticXL Cluster requires each platform to be after a Clean Install or restored to factory defaults.
- ElasticXL Cluster supports a maximum of:
  - 3 ElasticXL Cluster Members on each ElasticXL Site.
  - 6 ElasticXL Cluster Members in total.

  Note - If more Security Group Members are required, then use Maestro (*"Introduction to Maestro" on page 50*).
- ElasticXL Cluster requires at least 4 interfaces on each ElasticXL Cluster Member:
  - A dedicated management interface (the port "**Mgmt**" is selected automatically).
  - A dedicated sync interface (the port "**Sync**" is selected automatically).

    Important:
    - The "**Sync**" ports of all ElasticXL Cluster Members in the same ElasticXL Cluster must connect to the same Layer 2 broadcast domain (a dedicated Layer 2 switch, or a dedicated VLAN).
    - Only one ElasticXL Cluster is supported in the same Layer 2 broadcast domain (connecting Sync interfaces of different ElasticXL Clusters is not supported).
    - Configuring the Sync interface as VLAN Trunk is **not** supported.
    - ElasticXL Cluster sends all traffic over the Sync network in clear-text (non-encrypted).
    - ElasticXL Cluster automatically configures the IP address of the sync network to 192.0.2.0/24.
  - An "external" interface (you select and configure this interface).

    ElasticXL Cluster assigns a unicast MAC Address to these data interfaces.

    ElasticXL Cluster does not rename these data interfaces.
  - An "internal" interface (you select and configure this interface).

    ElasticXL Cluster assigns a unicast MAC Address to these data interfaces.

    ElasticXL Cluster does not rename these data interfaces.
- ElasticXL Cluster renames the physical interfaces on the appliances:

- The "**Mgmt**" interface becomes a subordinate interface in the Bond called "**magg1**".
- The "**Sync**" interface is renamed to "**eth1-Sync**" and becomes a subordinate interface in the Bond called "**Sync**".

Notes - Gaia OS does not show the bond interface "**Sync**" (or its subordinate interfaces) in Gaia Portal and in the Gaia Clish "`set`" commands. This is to prevent any changes to this infrastructure interface.

- On each ElasticXL Site, only one ElasticXL Cluster Member (the SMO) accepts all traffic and distributes this traffic to other ElasticXL Cluster Members (works like the Pivot member in the ClusterXL Load Sharing Unicast mode).
- ElasticXL Cluster supports only the "**General**" Distribution Mode to assign incoming traffic to cluster members on each ElasticXL (the Gaia gClish command "`set distribution configuration`"). See *"Working with the Distribution Mode" on page 554*.
- ElasticXL Cluster supports only the VSNext mode (the Traditional VSX mode is not supported). To configure the VSNext mode, you must enable it during the Gaia First Time Configuration Wizard on the first Security Appliance.

Getting Started with ElasticXL Cluster

Limitations

- Adding or removing an unassigned interface from a Sync bond resets the flags. As a result, ElasticXL detection is disrupted, and ElasticXL drops the packet.

ElasticXL Configuration

Part 1 - Installation of Appliances

Procedure

Refer to the Getting Started Guide for your Security Appliance in sk96246.

1. Install each Security Appliance in a rack.
2. Connect network cables to each Security Appliance.
   - The "**Sync**" ports on the Security Appliances must connect through a dedicated Layer 2 switch, or a dedicated VLAN.
   - Data ports on the Security Appliances must connect to your traffic networks.
3. Connect power cables to each Security Appliance.
4. Power on each Security Appliance.

Part 2 - Gaia First Time Configuration Wizard

Procedure

Important - You must run the First Time Configuration Wizard only on **one** of the Security Appliances.

1. Connect your computer to **one** of these Security Appliances to the "**Mgmt**" port.
2. On your computer, configure a static IPv4 address in the subnet **192.168.1.0 / 24**.

   Refer to the Getting Started Guide for your Security Appliance in sk96246.
3. In a web browser, enter this URL:

   ```
   https://192.168.1.1
   ```
4. The Gaia Portal login page opens.
5. Enter the default username and password: `admin` and `admin`.
6. Click **Login**.

The Gaia First Time Configuration Wizard opens.

For more information, see the *R82 Gaia Administration Guide* > Chapter "*Configuring Gaia for the First Time*" > Section "*Running the First Time Configuration Wizard in Gaia Portal*".

7. In the "**Welcome**" window:

   Click **Next**.

8. In the "**Deployment Options**" window:

   a. Select **Continue with R82 configuration**.

   b. Click **Next**.

9. In the "**Authentication Details**" window:

   Configure the main passwords for the Gaia OS.

   a. In the section "**Change the default administrator password**":

      Configure the password for the Expert mode.

   b. In the section "**Change the default password for Gaia maintenance mode**":

      Configure the password for the Maintenance Mode (GRUB).

      Best Practice - For security reasons, we recommend to configure a different passwords for the Expert mode and for the Maintenance Mode.

   c. Click **Next**.

   Note - You can change each password after you complete the Gaia First Time Configuration Wizard.

10. In the "**Management Connection**" window:

    In this window, you select and configure the main Gaia Management Interface.

    You connect to this IP address to open the Gaia Portal or CLI on the ElasticXL Cluster.

    a. Configure the applicable IPv4 and IPv6 settings.

    b. Click **Next**.

11. In the "**Internet Connection**" window, click **Next**.

    You must configure the required IP addresses on the ElasticXL Cluster interfaces after the First Time Configuration Wizard.

12. In the "**Device Information**" window:

a. Configure the desired hostname.

   For example: `ElasticXL_Cluster`

   - The hostname format for ElasticXL Cluster Members on the ElasticXL Site 1:

     `<Hostname>-s01-01`, `<Hostname>-s01-02`, `<Hostname>-s01-03`

   - The hostname format for ElasticXL Cluster Members on the ElasticXL Site 2:

     `<Hostname>-s02-01`, `<Hostname>-s02-02`, `<Hostname>-s02-03`

b. Configure the required DNS settings.

c. Configure the required Proxy settings.

d. Click **Next**.

13. In the "**Date and Time Settings**" window:

    a. Configure the required date and time settings.

    b. Click **Next**.

14. In the "**Installation Type**" window:

    a. Select **Security Gateway and/or Security Management**.

    b. Click **Next**.

15. In the "**Products**" window:

    a. In the **Products** section, select **Security Gateway**.

    b. In the **Clustering** section, select **Unit is a part of a cluster** and select **ElasticXL**.

    Important - To install this ElasticXL Cluster in the VSNext mode, in the **Gateway Virtualization** section, select **Install as VSNext**.
    You **cannot** convert to the VSNext mode after the installation.

    c. Click **Next**.

16. In the "**Secure Communication to Management Server**" window:

    a. Configure a one-time Activation Key.

    You must enter this key later in SmartConsole when you create the corresponding Security Gateway object and initialize SIC.

    b. Click **Next**.

17. In the "**First Time Configuration Wizard Summary**" window, click **Finish**.

18. The First Time Configuration Wizard performs the required steps and reboots this Security Appliance.
19. You now have a ElasticXL Cluster with one ElasticXL Cluster Member.
20. Connect to your ElasticXL Cluster at the IP address you configured in the "**Management Connection**" window.
21. Enter the username "`admin`" and the password you configured for the Expert mode in the "**Authentication Details**" window.

Part 3 - Configuration of ElasticXL Cluster

Procedure

1. Configure the applicable settings that require a reboot.

   Note - Do not change the SecureXL mode. It must run in the Kernel Mode (KPPAK).

   Best Practice - Do not to change the number of CoreXL Firewall instances. Use CoreXL Dynamic Balancing (enabled by default).

2. Install the required Hotfixes / Jumbo Hotfix Accumulator.
3. **Reboot** (only if you performed Step 1 and Step 2).
4. Configure the required IP addresses on the data interfaces, to which your networks must send their traffic.

   Refer to the *R82 Gaia Administration Guide* > Chapter "*Network Management*" > Section "*Network Interfaces*".

5. Configure the required static routes.

   Refer to the *R82 Gaia Administration Guide*:

   - Chapter "*Network Management*" > Section "*IPv4 Static Routes*".
   - Chapter "*Network Management*" > Section "*IPv6 Static Routes*".

Part 4 - Configuration in SmartConsole

Procedure

1. Configure a single Security Gateway object that represent this ElasticXL Cluster (this is the Single Management Object, SMO).
2. Configure and install the applicable Security Policies on this Security Gateway object.

Part 5 - Adding other ElasticXL Cluster Members

Add other ElasticXL Cluster Members to this ElasticXL, as needed.

The new ElasticXL Cluster Members automatically clone all software packages, settings, and security policies from the first ElasticXL Cluster Member (the SMO).

You can add other ElasticXL Cluster Members to an ElasticXL Cluster in Gaia Portal or in Gaia gClish.

Adding a new ElasticXL Cluster Member in Gaia Portal (recommended)

1. Connect to Gaia Portal on the ElasticXL Cluster.
2. In the left panel, click **Cluster Management**.
3. In the section **Cluster Gateways**, click **Pending Gateways**.
4. Select the required Security Appliance.
5. Select to which ElasticXL Site you want to add this Security Appliance:
   - **Add to the existing Site (configures Load Sharing with ...)**
   - **Create a new Site (configures High Availability with ...)**
6. Click **Add**.
7. In the notification popup, click **OK**.
8. Wait for the new Security Appliance to join this ElasticXL Cluster.

Adding a new ElasticXL Cluster Member in Gaia gClish

1. Connect to the command line on the ElasticXL Cluster.
2. Log in to Gaia gClish.
3. Get the list of the ElasticXL Cluster Members and detected Security Appliances:

   ```
   show cluster info provision
   ```

   See *"show cluster info" on page 967*

   The first Security Appliance has the state from "`CLUSTER_MEMBER`.

   The second Security Appliance has the state from "`REQUEST_TO_JOIN`.
4. Add the new Security Appliance to the required ElasticXL Site (existing Site or new Site):

   Note - See the example steps below.

   Syntax:

```
add cluster member
      method
            hostname identifier <Hostname>
            serial-number identifier <Serial Number>
            request-id identifier <Request ID>
      site-id {1 | 2}
      [format json]
```

Parameters:

Parameter	Description
`method`	Specifies how to identify an Security Appliance (press the Tab key to see the detected Security Appliances): ■ `hostname identifier <Hostname>` Adds the Security Appliance by its hostname ■ `serial-number identifier <Serial Number>` Adds the Security Appliance by its serial number ■ `request-id identifier <Request ID>` Adds the Security Appliance by its ElasticXL Request ID (as 32-bit string). This method allows a secure joining of a new Security Appliance. The "Request ID" is a hash of the public certificate key of the Security Appliance. An administrator can: a. Locate the new Security Appliance in a datacenter. b. Connect to the command line on the Security Appliance. c. Log in to Gaia Clish with default username and password: `admin` and `admin` (because we do not run the Gaia First Time Configuration Wizard on the additional Security Appliances that join the ElasticXL Cluster). d. Get the generated Request ID with this command: `show cluster member info [request-id]`
`site-id`	Specifies the ElasticXL Site ID, to which you add the Security Appliance - 1 or 2.
`format`	Specifies the output format - JSON (instead of the default table format).

Example:

a. Let us add the second Security Appliance to the new ElasticXL Site Site 2:

```
[Global] EXL-s01-01> add cluster member method request-id identifier
676190f4bc5b800b59f08c408942a484 site-id 2
Successfully added as member 2_1
[Global] EXL-s01-01
```

b. The second Security Appliance changes its state from "REQUEST_TO_JOIN" to "APPROVED_TO_JOIN".

c. After some time, the second Security Appliance changes its state from "APPROVED_TO_JOIN" to "JOINING_CLUSTER".

d. The second Security Appliance clones the required software packages and settings from the SMO, configures itself, and reboots.

This stage takes several minutes.

e. After the reboot, the second Security Appliance changes its state to "CLUSTER_MEMBER".

5. Monitor the progress on the SMO ElasticXL Cluster Member.

You can monitor the progress in Gaia gClish of ElasticXL Cluster with one of these commands:

insights
show cluster info provision [live]

See:

- *"insights" on page 903*.
- *"show cluster info" on page 967*

Monitoring the progress on the new ElasticXL Cluster Member

You can see how the new Security Appliance clones the software image from the SMO:

1. Connect your computer to the console port on the new Security Appliance.
2. Configure the terminal application on your computer.

   See *"insights" on page 903*.
3. Log in to Gaia Clish.

   Use the default username and password - `admin` and `admin`.
4. Run:

   ```
   insights
   ```
5. Watch the alerts.
6. When the configuration is complete, the new Security Appliance reboots.

Part 6 - Installing licenses on ElasticXL Cluster Members

Procedure for an ElasticXL Cluster in the Gateway mode

1. Connect an SSH client to the IP address of the ElasticXL Cluster.
2. Log in.
3. If you default shell is the Expert mode, then go to Gaia gClish:

   ```
   gclish
   ```

4. Get the MAC Addresses of the "**magg1**" interfaces from all ElasticXL Cluster Members and write them down:

   ```
   show interface magg1 mac-addr
   ```

   Example:

   ```
   [Global] EXL-s01-01> show interface magg1 mac-addr
   1_01:
   mac-addr XX:XX:XX:11:22:33

   1_02:
   mac-addr XX:XX:XX:44:55:66

   [Global] EXL-s01-01>
   ```

5. In *Check Point User Center*, generate a license for each Security Appliance using these parameters:

   a. IPv4 address of the ElasticXL Cluster.

      This is the IPv4 address of the "**Mgmt**" interface of the first ElasticXL Cluster Member, on which you ran the Gaia First Time Configuration Wizard.

   b. MAC Address of the "**magg1**" interface of **each** ElasticXL Cluster Member.

   Prepare the list of the required "`cplic put`" commands - for each generated license, you get an email from the User Center.

6. Connect an SSH client to the IP address of the ElasticXL Cluster.
7. Log in.
8. Run all the "`cplic put`" commands to install the licenses.

Procedure for an ElasticXL Cluster in the VSNext mode

1. Connect an SSH client to the IP address of the ElasticXL Cluster.
2. Log in.
3. If you default shell is Gaia gClish, then go to the Expert mode:

   ```
   expert
   ```

4. For Site 1, get the MAC Addresses of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 from **each** ElasticXL Cluster Member and write them down:

   a. Go to the context of the first ElasticXL Cluster Member on Site 1:

      ```
      member 1_1
      ```

   b. Get the MAC Address of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 and write it down:

      ```
      ip netns exec CTX00500 cat /sys/class/net/Mgmt/address
      ```

   c. Go to the context of the second ElasticXL Cluster Member on Site 1:

      ```
      member 1_2
      ```

   d. Get the MAC Address of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 and write it down:

      ```
      ip netns exec CTX00500 cat /sys/class/net/Mgmt/address
      ```

   e. Go to the context of the third ElasticXL Cluster Member on Site 1:

      ```
      member 1_3
      ```

   f. Get the MAC Address of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 and write it down:

      ```
      ip netns exec CTX00500 cat /sys/class/net/Mgmt/address
      ```

5. For Site 2 (if configured), get the MAC Addresses of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 from **each** ElasticXL Cluster Member and write them down:

a. Go to the context of the first ElasticXL Cluster Member on Site 2:

```
member 2_1
```

b. Get the MAC Address of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 and write it down:

```
ip netns exec CTX00500 cat /sys/class/net/Mgmt/address
```

c. Go to the context of the second ElasticXL Cluster Member on Site 2:

```
member 2_2
```

d. Get the MAC Address of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 and write it down:

```
ip netns exec CTX00500 cat /sys/class/net/Mgmt/address
```

e. Go to the context of the third ElasticXL Cluster Member on Site 2:

```
member 2_3
```

f. Get the MAC Address of the "**Mgmt**" interface from the default Virtual Switch object with the ID 500 and write it down:

```
ip netns exec CTX00500 cat /sys/class/net/Mgmt/address
```

6. In *Check Point User Center*, generate a license for **each** Security Appliance using these parameters:

   a. IPv4 address of the ElasticXL Cluster.

      This is the IPv4 address of the "**Mgmt**" interface of the first Security Appliance, on which you ran the Gaia First Time Configuration Wizard.

   b. MAC Address of the "**Mgmt**" interface of each Security Appliance as appeared in the CLI output in Step 4.

   Prepare the list of the required "`cplic put`" commands - for each generated license, you get an email from the User Center.

7. Connect an SSH client to the IP address of the ElasticXL Cluster.
8. Log in.
9. Run all the "`cplic put`" commands to install the licenses.

Removing a Cluster Member from ElasticXL Cluster

Note - When you remove a Cluster Member from ElasticXL Cluster, that Cluster Member returns to the clean version that was installed last. If that Cluster Member was upgraded, then it returns to the upgraded version.

You can remove ElasticXL Cluster Members from an ElasticXL Cluster in Gaia Portal or in Gaia gClish.

Procedure in Gaia Portal (recommended)

1. Connect to Gaia Portal on the ElasticXL Cluster.
2. In the left panel, click **Cluster Management**.
3. In the section **Cluster Gateways**, select the required Security Appliance.
4. From the top toolbar, click **Actions** and click **Delete**.
5. In the notification popup, click **OK** to confirm.

Procedure in Gaia Clish

1. Connect to the command line on the ElasticXL Cluster.
2. Log in to Gaia gClish.
3. Remove the Cluster Member:

```
delete cluster member method {hostname | serial-number | id}
<VALUE> [format json]
```

Moving an ElasticXL Cluster Member between ElasticXL Sites

You can move ElasticXL Cluster Members between ElasticXL Sites in Gaia Portal or in Gaia gClish.

Procedure

1. Remove the ElasticXL Cluster Member from the ElasticXL Cluster.
2. Add the pending Security Appliance to the required ElasticXL Site.

Installing and Uninstalling a Hotfix on ElasticXL Cluster

See *"Installing and Uninstalling a Hotfix on Security Group Members" on page 518*.

Troubleshooting Log Files

File	Description
`/var/log/lightshot.log`	Shows the information about: 1. Creation of a Gaia Lightshot snapshot on the SMO. 2. Image cloning from the SMO.
`$FWDIR/log/blade_config`	Show important messages about the cluster state changes from "down" to "up".
`/var/log/merge_license_file.log`	Shows the information about the license installation.

FAQ

- **Does ElasticXL Cluster support MAGG (bond of Mgmt interfaces)?**

  Yes - the default configuration is a Bond called "`magg1`" that contains the "`Mgmt`" interface of the Security Appliance.

- **Does ElasticXL Cluster support a bond of Sync interfaces?**

  Yes - the default configuration is a Bond called "`Sync`" that contains the `eth1-Sync` ("`Sync`") interface of the Security Appliance.

  By design, this interface is hidden.

- **Does ElasticXL Cluster support a migration from a ClusterXL configuration to a ElasticXL configuration?**

  Such a migration feature is on a roadmap.

- **Does ElasticXL Cluster support the Traditional VSX mode?**

  No.

  ElasticXL Cluster supports only the VSNext mode.

  See the *R82 VSX Administration Guide*.

  In the future, it is planned to support for the Traditional VSX mode only during a migration from a legacy VSX Cluster to an ElasticXL Cluster in the VSNext mode.

Working with Quantum Maestro

Note - This chapter describes the unique procedures that apply only to Maestro. For additional procedures that apply to all Scalable Platforms, see the chapter *"Common Procedures for Scalable Platforms" on page 504*.

Maestro Overview

Check Point Maestro introduces to the industry a new way to utilize current hardware investment and maximize appliance capacity in an easy-to manage HyperScale network security solution to bring our networks and data center to the world of hybrid clouds.

With Maestro, organizations can simplify their data center workflow orchestration and scale up their existing Check Point Security Gateways on demand - the same way as they can spin up new servers and compute resources in public clouds.

The Maestro HyperScale network security solution orchestrates multiple Quantum Security Gateways as one unified system, with seamless and near limitless scaling. Bring scale, agility, and elasticity of the cloud on premises with efficient N+1 clustering based on Check Point HyperSync technology. Maestro Orchestrators distribute internal and external network traffic equally across multiple Quantum Security Gateways managed as a single group with a common security feature set and policy. With Maestro, businesses of all sizes can have cloud scale and agility with datacenter resiliency - all while maximizing cost efficiency.

- Security at HyperScale:

  Up to 52 Gateways capable of 1.5 Tera/bps of Threat Prevention Performance (depends on the Orchestrator and Security Appliance models)

- Flexible Operations:

  Spin up new Security Gateways on demand to accommodate your dynamic security needs

- Cloud-Level Efficiency:

  Full active-active redundancy to completely utilize all your hardware resources

Maestro Security Groups

You can dynamically allocate or deallocate compute resources within and between Security Groups to meet your needs.

Each Security Group is a logical group of Security Appliances providing Active/Active cluster functionally segregated from other Security Groups.

Each Security Group has dedicated internal and external interfaces and may have a different configuration set and policy. For example, an Access Control Security Group protecting a data center, or a Threat Prevention Security Group providing perimeter protection.

Action Plan:

1. Connect Maestro Orchestrators on your network:
   a. Connect the sync ports between the Orchestrators (internal sync on the same Site, and external sync between the Sites).
   b. Connect the data networks to the Orchestrators (to uplink ports).
2. Connect Check Point Security Appliances to the Orchestrators (to downlink ports).
3. On **one** of the Orchestrators, configure the applicable Security Group.
4. In SmartConsole:
   a. Configure a single Security Gateway object (the Single Management Object, SMO) that represent this Security Group.
   b. Configure and install the applicable Security Policies on this Security Gateway object.
5. On the Security Group, configure other applicable settings (for example, routing).
6. Add other Security Appliances to the Security Group, as needed.

   The appliances automatically clone all software packages, settings, and security policies from the SMO Security Group Member.

For the initial installation and configuration, see the *Maestro Getting Started Guide*.

Introduction to Maestro

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 Maestro Orchestrator provides:

- Security of infinite scale.
- Redundancy - 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.

Note - To see the maximum numbers of supported items in Maestro, see the *R82 Release Notes* > Chapter "**Maximum Supported Items**".

Important Links

For more information and the software, see the R82 Home Page: sk181127.

- Read the R82 Known Limitations in sk181128.
- To learn about the differences between different Scalable Platform versions, see sk173183.
- Read sk180461 for information about Maestro licensing features.

Getting Started with Maestro

Workflow for Maestro:

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

   Follow the *Maestro Getting Started Guide*.

2. Get familiar with Security Group concepts:

   See:

   - *"Single Management Object and Policies" on page 535*
   - *"Policy Management on Security Group Members" on page 539*

3. Configure the required Security Groups in Maestro.

   See *"Configuring Security Groups in Maestro" on page 98*.

4. Learn how to monitor your Security Groups:

   See:

   - *"System Monitoring in Maestro" on page 214*
   - *"System Monitoring on Security Groups" on page 640*

5. Learn how to optimize your Security Groups:

   See:

   - *"System Optimization in Maestro" on page 217*
   - *"System Optimization on Security Groups" on page 636*

6. Learn how to install Hotfixes in Maestro:

   See:

   - *"Installing and Uninstalling a Hotfix on Maestro Orchestrators" on page 82*
   - *"Installing and Uninstalling a Hotfix on Security Group Members" on page 518*

7. Learn how to troubleshoot your Security Groups:

   See:

   - *"Troubleshooting in Maestro" on page 263*
   - *"Troubleshooting on Security Groups" on page 682*

Upgrading Maestro to R82

This section describes the steps for upgrading and rolling back a Maestro environment - the Maestro Orchestrators and the Security Groups.

For rollback procedures, see:

- *"Rolling Back a Failed Upgrade of a Maestro Orchestrator from R82" on page 79*
- *"Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC)" on page 505*

Upgrading Maestro Environment to R82

This section describes the steps for upgrading a Maestro environment (the Maestro Orchestrators and the Security Groups) with Zero Downtime - as a Multi-Version Cluster (MVC).

This procedure supports only these upgrade paths for Maestro Security Groups:

Source Version and Mode	Target Version and Mode
R81.20 in the Gateway mode	R82 in the Gateway mode
R81.20 in the Traditional VSX mode	R82 in the Traditional VSX mode
R81.10 in the Gateway mode	R82 in the Gateway mode
R81.10 in the Traditional VSX mode	R82 in the Traditional VSX mode

Important - See these rollback procedures:

- *"Rolling Back a Failed Upgrade of a Maestro Orchestrator from R82" on page 79*
- *"Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC)" on page 505*

Important - You can install the R82 Jumbo Hotfix Accumulator on a Security Group only after you complete the entire upgrade procedure. Before you install it, you must log out from all Gaia gClish sessions.

Important Notes for 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).
- To prevent traffic outage in an environment with two Orchestrators on a Single Site, make sure each Uplink interface and each Management interface are configured as a Bond interface.
  Example:
  - Bond interface `magg1` with the subordinate interfaces `eth1-Mgmt1` on `Orch1_1` and `eth2-Mgmt1` on `Orch1_2`.
  - Bond interface `bond2` with subordinate interfaces `eth1-05` on `Orch1_1` and `eth2-05` on `Orch1_2`.
- 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 Maestro Dual Site environment:

  Procedure

  1. Upgrade the Orchestrators on the Standby Site (for example, 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 that is configured on these Orchestrators.
     b. If your default shell is Gaia gClish (`/etc/gcli.sh`), then go to the Expert mode:

     ```
     expert
     ```

     c. Initiate a fail-over of all Security Group Members:

     ```
     chassis_admin -c <ID of non-upgraded Active Site> down
     ```

     ```
     chassis_admin -c <ID of non-upgraded 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 *R82 Installation and Upgrade Guide*.
- This procedure applies to Security Groups in the Gateway mode and the Traditional VSX mode.
  In Traditional VSX mode, you must run all the commands in the context of VS0:
  - To change the context in Gaia gClish, run: `set virtual-system 0`
  - To change the context in the Expert mode, run: `vsenv 0`
- **During the upgrade process, it is:**
  - **Forbidden to change the configuration of the Security Group and its Security Group Members.**
- 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	• 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.
Single Site	• 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 from 1_4 to 1_5.

Environment	Description
Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.

- 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 the Security Group.
    2. If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish:
       ```
       gclish
       ```
    3. Get the current Active/Standby mode and write it down (you need it at the end of the procedure):
       ```
       show chassis high-availability mode
       ```
       Available Modes:

Mode ID	Mode Title	Mode Description
0	**Active/Standby - Active Up**	No primary Site. The currently Active Site stays Active until one of these changes: ◦ The currently Active Site changes its state to "DOWN". If the formerly Active Site changes its state to "UP" again, it becomes the Standby Site. ◦ The quality grade of the currently Standby Site becomes greater than the quality grade of the currently Active Site.
1	**Active/Standby - Primary Up**	The Active Site always stays Active until one of these changes: ◦ The currently Active Site changes its state to "DOWN". If the formerly Active Site changes its state to "UP" again, it becomes the Active Site again. ◦ The quality grade of the currently Standby Site becomes greater than the quality grade of the currently Active Site.
2	Not available	Not supported. This mode is reserved.
3	**Standby Chassis VSLS Mode**	In the Traditional VSX mode, provides Virtual System Load Sharing.

4. Decide which of the Site should be Active for this procedure.
5. Change the Active/Standby mode to "**Active/Standby - Primary Up**" (value "1"):

```
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 Standby Site, change the Active/Standby mode to "**Active/Standby - Primary Up**" (value "1"):

```
set cluster configuration high-availability
mode 1
```

9. On the upgraded Site change the Site Priority - enter the number of the currently Active Site:

```
set cluster configuration high-availability
vs site_priority {1 | 2}
```

10. Upgrade all Security Group Members on the new Standby Site (former Active Site).
11. Change the Active/Standby mode to the previous mode:

```
set cluster configuration high-availability
mode <Mode ID>
```

Required software packages:

Download the required software packages from sk181127:

1. The required CPUSE Deployment Agent.
2. The required Take of the Jumbo Hotfix Accumulator for the current version.
3. The R82 Upgrade Package for Scalable Platforms.

Workflow:

1. On the Management Server - Upgrade to the required version that can manage an R82 Security Group (see sk113113).
2. On the Orchestrator - Upgrade to R82 and install the R82 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 R82 (using two logical groups of Security Group Members).
7. In SmartConsole, install the policy.

Procedure:

Step 1 - Upgrade the Management Server

Upgrade the Security Management Server / Multi-Domain Security Management Server to the required version that can manage an R82 Security Group.

See the *R82 Release Notes* or sk113113.

Step 2 - On the Maestro Orchestrator, upgrade to R82 and install the R82 Jumbo Hotfix Accumulator

For more information about the CPUSE Deployment Agent, see sk92449.

Instructions for the CPUSE Deployment Agent - New CPUSE GUI

Step	Instructions
A	If the Orchestrator runs R80.20SP, then install the R80.20SP Jumbo Hotfix Accumulator Take 326 or higher on the Orchestrator.
B	In the Orchestrator's Gaia Portal, from the left tree, go to **Software Updates** > **Available Updates**.
C	In the top left, click **Add package** > **Upload package from local**.
D	In the **Import package** window, click **Browse for a file**.
E	Go to the folder where you put the *R82 Upgrade Package for Scalable Platforms* from sk181127.
F	Select the *R82 Upgrade Package for Scalable Platforms*.
G	Click **Open**.
H	Click **Import**.
I	A new row appears in the section **Major Versions**.
J	In the row of the imported R82 CPUSE Offline Package, click the **Verify** button.
K	In the row of the imported R82 CPUSE Offline Package, click the **Upgrade** button. **Important:** ■ Do **not** click the 3-dot menu and do **not** click **Clean install** because it performs a clean install, which deletes all configuration and reboots all Security Group Members). ■ At the end of the upgrade, the Orchestrator reboots automatically.
L	Install the Recommended Take of the R82 Jumbo Hotfix Accumulator. See *"Installing and Uninstalling a Hotfix on Maestro Orchestrators" on page 82*.

Instructions for the CPUSE Deployment Agent - Legacy CPUSE GUI

Step	Instructions
A	If the Orchestrator runs R80.20SP, then install the R80.20SP Jumbo Hotfix Accumulator Take 326 or higher on the Orchestrator.
B	In the Orchestrator's Gaia Portal, from the left tree, go to **Upgrades (CPUSE)** > **Status and Actions**.
C	In the top right section, click **Import Package**.
D	Click **Browse**.
E	Go to the folder where you put the *R82 Upgrade Package for Scalable Platforms* from sk181127.
F	Select the *R82 Upgrade Package for Scalable Platforms*.
G	Click **Open**.
H	Click **Import**.
I	Above the list of packages, near the help icon, click the filter button that currently says "**Showing Recommended packages**" and click "**All**". The filter must change to "**Showing All packages**".
J	Right-click the imported R82 CPUSE Offline Package and click **Verify Update**.
K	Right-click the imported R82 CPUSE Offline Package and click **Upgrade**. **Important:** ■ Make sure to click **Upgrade** (do **not** click **Install** because it performs a clean install, which deletes all configuration and reboots all Security Group Members). ■ At the end of the upgrade, the Orchestrator reboots automatically.
L	Install the Recommended Take of the R82 Jumbo Hotfix Accumulator. See *"Installing and Uninstalling a Hotfix on Maestro Orchestrators" on page 82*.

Step 3 - On the Management Server, change the version of the Traditional VSX Gateway object

Important - This step applies **only** when the Security Group works in the Traditional 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: `mdsenv <IP Address or Name of Domain Management Server>`
D	Upgrade the version of a VSX Gateway object in the management database: **Warning** - Make sure to close all SmartConsole clients connected to this Management Server. `vsx_util upgrade [-s <Mgmt Server>] [-u <UserName>]` For more information, see the *R82 VSX Administration Guide* > Chapter "Command Line Reference" > Section "vsx_util".
E	Log in with the Management Server administrator credentials.
F	Select the Traditional VSX Gateway object for this Security Group.
G	Change the version to **R82**. Follow the instructions on the screen.

Step 4 - 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set smo image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show smo image auto-clone state`

Step 5 - 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 sk181127:

- On a Maestro Security Group:

  "Installing a Hotfix Package on Security Group Members" on page 519

- On a Scalable Chassis:

  "Installing and Uninstalling a Hotfix on SGMs on Scalable Chassis" on page 317

Step 6 - 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 required CPUSE Deployment Agent package (from sk92449) 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 Gaia gClish (`/etc/gcli.sh`), then go to the Expert mode: `expert`
D	Make sure the CPUSE Deployment Agent package exists: `ls -l /<Full Path>/<Name of CPUSE Deployment Agent Package>`

E	Upgrade the CPUSE Deployment Agent:
	`update_sp_da /<Full Path>/<Name of CPUSE Deployment Agent Package>`
	Example:
	`update_sp_da /var/log/DeploymentAgent_XXXXXXXXX.tgz`

F	Make sure all Security Group Members have the same build of the CPUSE Deployment Agent: `gclish -c "show installer status build"`

Step 7 - On the Security Group, import the R82 upgrade package

Step	Instructions
A	Make sure you have the applicable CPUSE Offline package: *R82 Upgrade Package for Scalable Platforms*
B	Transfer the CPUSE Offline package to the Security Group (into some directory, for example `/var/log/`).
C	Connect to the command line on the Security Group.
D	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`
E	If you enabled MDPS (sk138672) on the Security Group, then go to the Management Plane: `set mdps environment mplane`

F	Import the CPUSE Offline package from the hard disk:
	`installer import local /<Full Path>/<Name of the CPUSE Offline Package>`
	Example:
	`[Global] HostName-s01-01 > installer import local /var/log/Check_Point_R82_Gaia_Install_and_Upgrade.tar`

G	Show the imported CPUSE packages: `show installer packages imported`

Step	Instructions

H	Make sure the imported CPUSE package can be installed on this Security Group:
	`installer verify [Press Tab]`
	`installer verify <Number of CPUSE Package> member_ids all`
	Example:
	`[Global] HostName-s01-01 > 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-s01-01 >`

Step 8 - On the Security Group, upgrade the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**A**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**B**" **over SSH**.

B	Go to the context of one of the Security Group Members in the Logical Group "A":
	`member <Member ID>`
	Example:
	`member 1_1`

C	If your default shell is Gaia gClish (`/etc/gcli.sh`), then go to the Expert mode: `expert`

D	Set the Security Group Members in the Logical Group "A" to the state "`DOWN`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "`g_clusterXL_admin`" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "A"> down`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "A"> down`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_1 down`
	`g_clusterXL_admin -b 1_2 down`
	`g_clusterXL_admin -b 1_3 down`
	`g_clusterXL_admin -b 1_4 down`

Step	Instructions
E	Examine the state of the Security Group Members: `asg monitor` The state of the Security Group Members must be: ■ In the Logical Group "**A**" - "**DOWN**". ■ In the Logical Group "**B**" - "**ACTIVE**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

F	Go from the Expert mode to Gaia gClish:
	■ If your default shell is the Expert mode (`/bin/bash`), then run:
	`gclish`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`), then run:
	`exit`

G	Upgrade the Security Group Members in the Logical Group "A":
	`installer upgrade [Press the Tab key]`
	`installer upgrade <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] HostName-s01-01 > 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) y`
	`[Global] HostName-s01-01 >`

Step	Instructions

H	Go from Gaia gClish to the Expert mode:
	■ If your default shell is the Expert mode (`/bin/bash`), then run:
	`exit`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`), then run:
	`expert`

I	Monitor the Security Group Members in the Logical Group "A" until they boot: `asg monitor` **Important:** ■ By design, the upgraded Security Group Members boot into the state "**DOWN(Policy)(R82)**" because the Critical Device "**Policy**" reports its state as "`problem`" (you can run the "`cluster-cli show info pnotes`" command). ■ In the Traditional VSX mode, the Security Group Members are pulling the policy automatically from Management Server during their boot. **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

Step 9 - In SmartConsole, change the version of the Security Gateway object

Note - This step applies only to a Security Group in the Gateway mode.

Warning - This step does **not** apply when the Security Group works in the Traditional VSX mode.
In the Traditional 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 **Gateways & Servers**.
C	Double-click the Security Gateway object for this Security Group.
D	In the left tree, click **General**.
E	In the **Version** field, select **R82**.
F	Click **OK**.
G	Publish the session.
H	Install the Access Control policy on this Security Gateway object. **Important** - You must **disable** the Accelerated Policy Installation as described in sk168055: i. Click **Install Policy**. ii. In the **Install Policy** window, right-click on the Security Gateway object. iii. Select **Do not use Install Policy Acceleration for all gateways**. iv. Select the Security Gateway object. v. Click **Install**. **Notes:** ■ Only the upgraded R82 Security Group Members install this policy. The Security Group Members that still run the previous version ignore this policy installation. ■ If the policy installation fails, refer to sk184660.

Step	Instructions
I	On the Security Group (in the Expert mode), examine the state of the Security Group Members: `asg monitor` The state of the Security Group Members must be: ■ In the upgraded Logical Group "**A**" - "**DOWN(READY)(R82)**". ■ In the Logical Group "**B**" - "**ACTIVE(<previous version>)**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

Step 10 - On the Security Group, change the state of Security Group Members in the Logical Group "A" to "Up"

Step	Instructions

A	Set the Security Group Members in the Logical Group "A" to the state "`UP`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "`g_clusterXL_admin`" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "A"> up`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "A"> up`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_1 up`
	`g_clusterXL_admin -b 1_2 up`
	`g_clusterXL_admin -b 1_3 up`
	`g_clusterXL_admin -b 1_4 up`

B	Examine the state of the Security Group Members: `asg monitor` The state of the Security Group Members must be: ■ In the upgraded Logical Group "**A**" - "**ACTIVE(R82)**". ■ In the Logical Group "**B**" - "**ACTIVE(<previous version>)**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

Note - Because of the Multi-Version Cluster (MVC) mechanism design, the upgraded Security Group Members also process the traffic.

Important - If this Security Group works in the Traditional VSX mode, the state of the upgraded Security Group Members may remain "**DOWN**" because the Critical Device "`DSD`" reports its state as "`problem`" (run the "`show cluster info pnotes`" command).
This issue may occur if before the upgrade you configured **static** CoreXL Affinity with the command "`fw ctl affinity -s -d -fwkall <Number of CPUs>`" (to see the current configuration, run the command "`fw ctl affinity -l -x`").
Follow these workaround steps:

1. Connect to the command line on the Security Group.
2. If the default shell is the Expert mode, then go to Gaia gClish:

   ```
   gclish
   ```

3. Disable the CoreXL Dynamic Balancing:

   ```
   set dynamic-balancing state disable
   ```

4. Reboot the upgraded Security Group Members:

   ```
   reboot -b <SGM IDs>
   ```

5. Examine the state of the upgraded Security Group Members:

   ```
   show cluster info pnotes
   ```

   ```
   asg monitor
   ```

Step 11 - On the Security Group, change the state of Security Group Members in the Logical Group "B" to "Down"

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: ■ Connect to one of the Security Group Members in the Logical Group **"B" through the console**. ■ Connect to one of the Security Group Members in the Logical Group **"A" over SSH**.

B	Set the Security Group Members in the Logical Group "B" to the state "DOWN":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "g_clusterXL_admin" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "B"> down`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "B"> down`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_5 down`
	`g_clusterXL_admin -b 1_6 down`
	`g_clusterXL_admin -b 1_7 down`
	`g_clusterXL_admin -b 1_8 down`

Note - At this time, the Security Group runs only with the upgraded Security Group Members.
You can perform the required tests on your network to make sure the new version works as expected.
If there are any issues:

1. Set the Security Group Members in the Logical Group "B" to the state "UP".
2. Set the Security Group Members in the upgraded Logical Group "A" to the state "DOWN".

Step 12 - On the Security Group, upgrade the Security Group Members in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**B**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**A**" **over SSH**.

B	Go to the context of one of the Security Group Members in the Logical Group "B":
	`member <Member ID>`
	Example:
	`member 1_5`

C	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`

D	Upgrade the Security Group Members in the Logical Group "B":
	`installer upgrade [Press the Tab key]`
	`installer upgrade <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] HostName-s01-01 > 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) y`
	`[Global] HostName-s01-01 >`

E	Go from Gaia gClish to the Expert mode:
	■ If your default shell is the Expert mode (`/bin/bash`), then run:
	`exit`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`), then run:
	`expert`

Step	Instructions
F	Monitor the Security Group Members in the Logical Group "B" until they boot: `asg monitor` The state of the Security Group Members must be: ■ In the Logical Group "**A**" - "**ACTIVE(R82)**". ■ In the Logical Group "**B**" - "**DOWN(READY)(R82)**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

G	Set the Security Group Members in the Logical Group "B" to the state "`UP`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "`g_clusterXL_admin`" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "B"> up`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "B"> up`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_5 up`
	`g_clusterXL_admin -b 1_6 up`
	`g_clusterXL_admin -b 1_7 up`
	`g_clusterXL_admin -b 1_8 up`

Step 13 - 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 Gaia gClish (`/etc/gcli.sh`), then go to the Expert mode: `expert`
C	Examine the state of the Security Group Members: `asg monitor` Each Security Group Members must have the state "**ACTIVE**".
D	Run this command (see *"hcp" on page 899*): `hcp -m all -r all`

Rolling Back a Failed Upgrade of a Maestro Orchestrator from R82

This section describes the steps for rolling back a failed upgrade of a Maestro Orchestrator to R82.

Warning - If after an upgrade of the Orchestrator to R82 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 R82, then **before** you revert the Orchestrator, you must revert all Security Groups.
  Follow this procedure - *"Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC)" on page 505*:
- 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 on each Site.
- In a Dual Site environment:
  1. In each Security Group, perform a failover of all Security Group Members from one Site (for example, Site 2) to another Site (for example, Site 1).
     - To monitor the state of a Security Group, see *"asg stat" on page 829*.
     - To perform a failover in a Security Group on an entire Site, see *"set cluster site-id <Site ID> admin-state" on page 939*.
  2. Perform this rollback procedure on each Orchestrator on the site, from which you failed over all Security Group Members.
     In our example, perform this rollback procedure on each Orchestrator on Site 2.
  3. In each Security Group, perform a failover of all Security Group Members from their current Site to the reverted Site.
     In our example, perform this failover from Site 1 to Site 2.
  4. Perform this rollback procedure on each Orchestrator on the site, from which you failed over all Security Group Members.
     In our example, perform this rollback procedure on each Orchestrator on Site 1.

Procedure for each Orchestrator:

Step	Instructions
1	Connect to the command line on the Orchestrator (in our example, "Orchestrator 1_1").

Step	Instructions
2	If your default shell is Gaia Clish (`/etc/cli.sh`), then go to the Expert mode: `expert`
3	Stop the Orchestrator service: `orchd stop` **Warning** - This immediately stops all traffic through Security Groups running on this Orchestrator.

4	Go from the Expert mode to Gaia Clish:
	■ If your default shell is the Expert mode (`/bin/bash`), then run:
	`clish`
	■ If your default shell is Gaia Clish (`/etc/cli.sh`), then run:
	`exit`

5	Restore the Gaia snapshot, which was created automatically during the upgrade: `set snapshot revert`**`[Press Space][Press Tab]`** The Orchestrator automatically reboots and starts the revert. For more information, see the *R82 Gaia Administration Guide* > Chapter *Maintenance* > Section *Snapshot Management*.
6	Wait for the reverted Orchestrator to boot.
7	Configure the same date and time settings on all other Orchestrators in your environment. For more information, see the *R82 Gaia Administration Guide* > Chapter *System Management* > Section *Time*.

Step	Instructions

8	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):
	■ In a Single Site environment:
	`ping 1_2`
	■ In a Dual Site environment:
	`ping 1_2`
	`ping 2_1`
	`ping 2_2`

9	Make sure the Security Group Members can pass traffic to each other:
	a. Connect to the command line on the Security Group.
	b. If your default shell is Gaia gClish (`/etc/gclish`), then go to the Expert mode:
	`expert`
	c. Examine the cluster state of the Security Group Members.
	On the SMO Security Group Member, run:
	`cphaprob state`
	The output must show that all Security Group Members are active.
	d. Send pings between Security Group Members:
	i. Connect to one of the Security Group Members
	(in our example, we connect to the first one - "1_1"):
	`member 1_1`
	ii. 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"):
	■ In a Single Site environment:
	`ping 1_2`
	■ In a Dual Site environment:
	`ping 1_2`
	`ping 2_2`

Step	Instructions
10	On each Security Group Member, make sure all links are up in the Security Group: a. Connect to the command line on the Security Group. b. Log in to Gaia gClish. c. Examine the state of links: `show cluster info interfaces` See *"show cluster info" on page 967*.

Installing and Uninstalling a Hotfix on Maestro Orchestrators

You use the **CPUSE** on each Maestro Orchestrator to install the applicable hotfixes.

Note - For Security Group Members, see *"Installing and Uninstalling a Hotfix on Security Group Members" on page 518*.

Important:

- For the **CPUSE** instructions, see sk92449.
- Jumbo Hotfix Accumulator reboots the Orchestrator after you install or uninstall it.
- Orchestrator stops processing traffic from the start of the Jumbo Hotfix Accumulator installation or uninstall and until Orchestrator comes up after the reboot.
- You must install the same Take of Jumbo Hotfix Accumulator on all Orchestrators on all Maestro Sites.

Installing a Hotfix Package on Orchestrators

Internet Connection	Installation Methods	Action Plan
Orchestrator **is** connected to the Internet	You can perform only an offline installation.	See the instructions for an Orchestrator that is **not** connected to the Internet.

Internet Connection	Installation Methods	Action Plan
Orchestrator is **not** connected to the Internet	You can perform only an offline installation.	**To install a CPUSE package in Gaia Portal** 1. Use the computer, from which you connect to Gaia Portal on the Orchestrator. 2. Download the applicable CPUSE Software Package from the *Check Point Support Center*. 3. Connect to Gaia Portal on each Orchestrator. 4. Import the applicable CPUSE Software Package. 5. Verify the applicable CPUSE Software Package. 6. Install the applicable CPUSE Software Package. **To install a CPUSE package in Gaia Clish** 1. Use the computer, from which you connect to Gaia Clish on the Orchestrator. 2. Download the applicable CPUSE Software Package from the *Check Point Support Center*. 3. Transfer the applicable CPUSE Offline Software Package to each Orchestrator to some directory (for example, `/var/log/path_to_CPUSE_packages/`). Make sure to transfer the CPUSE packages in the binary mode. 4. Connect to the command line on each Orchestrator and log in to Gaia Clish. 5. Import the applicable CPUSE Software Package. 6. Verify the applicable CPUSE Software Package. 7. Install the applicable CPUSE Software Package.

Uninstalling a Hotfix Package on Orchestrators

To uninstall a CPUSE package in Gaia Portal

1. Connect to Gaia Portal on each 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 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 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 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 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>
```

Authentication between Maestro Orchestrators

Warnings:

- To avoid synchronization issues between Orchestrators, do **not** configure Security Groups before making sure all Orchestrators are authenticated.
- Make sure only one administrator configures the authentication between Orchestrators at any time.
  This prevents an issue when different administrators configure the authentication on different Orchestrators.

Important - After you configure authentication between Orchestrators, you must configure it again in these cases:

- One of the Orchestrators was installed from scratch (clean install) or restored to factory defaults.
- An existing authenticated Orchestrator was replaced with another Orchestrator.
- Site ID or Orchestrator ID changed on an existing authenticated Orchestrator.

Introduction

Starting in R82, you can configure mutual authentication between all Maestro Orchestrators on your Maestro Sites to make sure their communication is secure and encrypted over Internal Sync ports (sync in the same Maestro Site) and External Sync ports (sync between Maestro Sites).

This authentication is based on SSH keys and SSL certificates. These SSL certificates are valid for one year. Orchestrators renew these SSL certificates automatically.

This authentication is a two-way mesh process - each Orchestrator authenticates all other Orchestrators.

Explanation for a Dual Site Maestro configuration:

Site	Orchestrator	Authentication with other Orchestrators
1	1_1	■ 1_2 ■ 2_1 ■ 2_2
	1_2	■ 1_1 ■ 2_1 ■ 2_2

Site	Orchestrator	Authentication with other Orchestrators
2	2_1	▪ 1_1 ▪ 1_2 ▪ 2_2
	2_2	▪ 1_1 ▪ 1_2 ▪ 2_1

Note - This popup appears when you connect to Gaia Portal on an Orchestrator, and not all Orchestrators are authenticated in this Maestro environment:

```
<Number> orchestrators are pending authentication, would
you like to authenticate them now?
```

If you click **Yes**, the **Authentication** window opens.

Authentication statuses in Gaia Portal and CLI

Status	Description
Authenticated	The local Orchestrator that shows this status has authenticated the remote Orchestrator.
Unknown	The local Orchestrator that shows this status cannot determine the status for the remote Orchestrator.
Unreachable	The local Orchestrator that shows this status cannot connect to the remote Orchestrator over the External Sync port (between Maestro Sites) or over the Internal Sync port (on the same Maestro Site).
Untrusted	The local Orchestrator that shows this status does not trust the remote Orchestrator.

Configuring new authentication between Maestro Orchestrators

The procedure below is for a Dual Site Maestro environment with four Orchestrators.

The same steps apply in a Single Site Maestro environment with two Orchestrators.

Configuring new authentication in Gaia Portal (recommended)

Important:
If you enabled Two-Factor Authentication in Gaia settings on Orchestrators, then before you establish trust between Orchestrators, you **must disable** the Two-Factor Authentication in Gaia settings on each Orchestrator.
After you establish trust between Orchestrators, enable the Two-Factor Authentication again in Gaia settings on Orchestrators.

Step	Instructions
1	Verify the fingerprint of each Orchestrator in one of these ways: ■ To verify the fingerprint of an Orchestrator in Gaia Portal: a. Connect to Gaia Portal of the Orchestrator. b. In the left panel, click **Orchestrator Management** > **Security Groups**. c. In the top right corner, click **Authentication**. d. In the section **Orchestrator ID: X_Y (local)**, refer to the field **Fingerprint**. ■ To verify the fingerprint of an Orchestrator in Gaia Clish: a. Connect to the command line on the Orchestrator. b. Log in to Gaia Clish. c. Run: `show ssh pubkey host localhost`
2	Connect to Gaia Portal on **one** of the Orchestrators. For example, Orchestrator **1_1**.
3	In the left panel, click **Orchestrator Management** > **Security Groups**.
4	In the top right corner, click **Authentication**.

Step	Instructions
5	In the section **Orchestrator ID: 1_2**: a. Click **Trust**. b. In the **Trust Orchestrator** window, click **Yes**. c. In the **Admin Password Required** window, enter the Expert mode password and click **OK** to approve the connection. This password is only used for the initial authentication process and is not stored after the authentication process completes. d. In the **Authentication Summary**, click **OK**. This establishes trust: ■ between 1_2 and 1_1.
6	In the section **Orchestrator ID: 2_1**: a. Click **Trust**. b. In the **Trust Orchestrator** window, click **Yes**. c. In the **Admin Password Required** window, enter the Expert mode password and click **OK** to approve the connection. This password is only used for the initial authentication process and is not stored after the authentication process completes. d. In the **Authentication Summary** window, click **OK**. This establishes trust: ■ between 2_1 and 1_1. ■ between 2_1 and 1_2.
7	In the section **Orchestrator ID: 2_2**: a. Click **Trust**. b. In the **Trust Orchestrator** window, click **Yes**. c. In the **Admin Password Required** window, enter the Expert mode password and click **OK** to approve the connection. This password is only used for the initial authentication process and is not stored after the authentication process completes. d. In the **Authentication Summary** window, click **OK**. This establishes trust: ■ between 2_2 and 1_1. ■ between 2_2 and 1_2. ■ between 2_2 and 2_1.

Step	Instructions
8	If you established trust with a new Orchestrator that was added to an existing Maestro environment, then on that new Orchestrator, run in the Expert mode: `orchd restart`

Configuring new authentication in CLI (Gaia Clish or Expert mode)

Important:
If you enabled Two-Factor Authentication in Gaia settings on Orchestrators, then before you establish trust between Orchestrators, you **must disable** the Two-Factor Authentication in Gaia settings on each Orchestrator.
After you establish trust between Orchestrators, enable the Two-Factor Authentication again in Gaia settings on Orchestrators.

Step	Instructions
1	Verify the fingerprint of each Orchestrator in one of these ways: ■ To verify the fingerprint of an Orchestrator in Gaia Portal: a. Connect to Gaia Portal of the Orchestrator. b. In the left panel, click **Orchestrator Management** > **Security Groups**. c. In the top right corner, click **Authentication**. d. In the section **Orchestrator ID: X_Y (local)**, refer to the field **Fingerprint**. ■ To verify the fingerprint of an Orchestrator in Gaia Clish: a. Connect to the command line on the Orchestrator. b. Log in to Gaia Clish. c. Run: `show ssh pubkey host localhost`
2	Connect to the command line on **one** of the Orchestrators. For example, Orchestrator **1_1**

Step	Instructions

3	Establish trust with the "`establish_mho_authentication`" command.
	Note - You can run this command in Gaia Clish or in the Expert mode.
	To see the built-in help, run:
	`establish_mho_authentication -h`
	To establish trust between all Orchestrators, run:
	`establish_mho_authentication all`
	To establish trust between the current Orchestrator and the specified Orchestrators, run
	(enter the required IDs separated by commas without spaces):
	`establish_mho_authentication 1_1,1_2,2_1,2_2`

Forcing existing authentication between Maestro Orchestrators

This action is helpful in these cases:

- You revoked trust with an Orchestrator and need to establish trust again.
- There are communication issues between authenticated Orchestrators.

Forcing existing authentication in Gaia Portal (recommended)

Step	Instructions
1	Connect to Gaia Portal on **one** of the Orchestrators.
2	In the left panel, click **Orchestrator Management** > **Security Groups**.
3	In the top right corner, click **Authentication**.
4	In the card of each Orchestrator, click ⋮ > click **Force Re-authentication**.
5	In the **Refresh Authentication** window, click **Yes**.

Forcing existing authentication in CLI (Gaia Clish or Expert mode)

Step	Instructions
1	Connect to the command line on **one** of the Orchestrators.

3	Establish trust with the "`establish_mho_authentication`" command.
	Note - You can run this command in Gaia Clish or in the Expert mode.
	To see the built-in help, run:
	`establish_mho_authentication -h`
	To establish trust between all Orchestrators, run:
	`establish_mho_authentication all`
	To establish trust between the current Orchestrator and the specified Orchestrators, run (enter the required IDs separated by commas without spaces):
	`establish_mho_authentication 1_1,1_2,2_1,2_2`

Step	Instructions
4	If you established trust with a new Orchestrator that was added to an existing Maestro environment, then on that new Orchestrator, run in the Expert mode: `orchd restart`

Revoking existing authentication between Maestro Orchestrators

Warning - For security reasons, perform this procedure **before** you remove an authenticated Orchestrator from the Maestro environment.

This procedure revokes the existing authentication of the selected Orchestrator on all other Orchestrators.

The example procedures below are for revoking trust with the Orchestrator **1_2**.

Option 1 - Revoking trust with a specific Orchestrator on all Orchestrators (recommended)

Step	Instructions
1	Connect to Gaia Portal on the Orchestrator **1_1**. (You can connect to any Orchestrator that will remain in this Maestro environment.)
2	In the left panel, click **Orchestrator Management** > **Security Groups**.
3	In the top right corner, click **Authentication**.
4	In the section **Orchestrator ID: 1_2**, click ⋮ > click **Revoke from all**.
5	In the **Revoke Orchestrator 1_2** window, click **Yes**.
6	In the **Authentication Summary** window, click **OK**.

Option 2 - Revoking trust with a specific Orchestrator only on one Orchestrator - in Gaia Portal

Part 1 of 2 - Revoking trust on Orchestrator 1_1

This step revokes trust on Orchestrator 1_1 with Orchestrator 1_2.

(You can connect to any Orchestrator that will remain in this Maestro environment.)

Step	Instructions
1	Connect to Gaia Portal on the Orchestrator **1_1**.
2	In the left panel, click **Orchestrator Management** > **Security Groups**.
3	In the top right corner, click **Authentication**.
4	In the section **Orchestrator ID: 1_2**, click ⋮ > click **Revoke**.

Step	Instructions
5	In the **Revoke Orchestrator 1_2** window, click **Yes**.
6	In the **Authentication Summary** window, click **OK**.

Part 2 of 2 - Revoking trust on Orchestrator 1_2

This step revokes trust on Orchestrator 1_2 with all other Orchestrators:

Step	Instructions
1	Connect to Gaia Portal on the Orchestrator **1_2**.
2	In the left panel, click **Orchestrator Management** > **Security Groups**.
3	In the top right corner, click **Authentication**.
4	In the section **Orchestrator ID: 1_1**: a. Click **Revoke**. b. In the **Revoke Orchestrator 1_1** window, click **Yes**. c. In the **Authentication Summary** window, click **OK**.
5	In the section **Orchestrator ID: 2_1**: a. Click **Revoke**. b. In the **Revoke Orchestrator 2_1** window, click **Yes**. c. In the **Authentication Summary** window, click **OK**.
6	In the section **Orchestrator ID: 2_2**: a. Click **Revoke**. b. In the **Revoke Orchestrator 2_2** window, click **Yes**. c. In the **Authentication Summary** window, click **OK**.

Option 3 - Revoking trust with a specific Orchestrator only on one Orchestrator - in Gaia Clish

Part 1 of 2 - Revoking trust on Orchestrator 1_1

This step revokes trust on Orchestrator 1_1 with Orchestrator 1_2.

Step	Instructions
1	Connect to the command line on the Orchestrator **1_1**.

Step	Instructions
2	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia Clish: `clish`
3	Revoke trust with Orchestrator 1_2: `delete maestro authenticated mho 1_2`
4	Save the changes: `save config`

Part 2 of 2 - Revoking trust on Orchestrator 1_2

This step revokes trust on Orchestrator 1_2 with Orchestrator 1_1:

Step	Instructions
1	Connect to the command line on the Orchestrator **1_2**.
2	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia Clish: `clish`
3	Revoke trust with Orchestrator 1_1: `delete maestro authenticated mho 1_1`
4	Save the changes: `save config`

Blocking authentication with a Maestro Orchestrator

This procedure configures the selected Orchestrator as untrusted.

You can do this to prevent an untrusted Orchestrator from accidentally becoming trusted in the future.

Procedure

Step	Instructions
1	Connect to Gaia Portal on **one** of the Orchestrators.
2	In the left panel, click **Orchestrator Management** > **Security Groups**.
3	In the top right corner, click **Authentication**.
4	In the applicable Orchestrator card, click **Do not trust**. The fingerprint is added to this file: `/etc/blocked_fingerprints`
5	In the **Block fingerprint** window, click **Yes** to confirm.
6	To unblock: a. Click the section **Untrusted Orchestrators** to expand it. b. In the applicable line, click **Trust**. c. In the **Unblock fingerprint** window, click **Yes** to confirm.

Troubleshooting

1. Run the "`orch_stat`" command:

Step	Instructions
1	Connect to the command line on each Orchestrator.
2	Log in to the Expert mode.
3	Run the command: `orch_stat -Av`

2. Run the HealthCheck Point (HCP) tool (see sk171436) and refer to the test "**Maestro Orchestrator Authentication**":

Step	Instructions
1	Connect to the command line on each Orchestrator.
2	Log in to the Expert mode.
3	Run the test: `hcp -r "Maestro Orchestrator Authentication"`
4	View the detailed report: `hcp --show-last`

Configuring Security Groups in Maestro

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

General Workflow in Maestro

Notes:

- It is assumed that you already installed the Maestro Orchestrators, the Security Appliances, and connected all cables. See the *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 *R82 Gaia Administration Guide* > Chapter "**System Management**" > Section "**System Passwords**".
- Conversion of an existing Security Gateway object (with the established SIC) to a Traditional VSX Gateway object is not supported.

Important - You must make sure that only **one** Security Group Member is "Active" in the Security Group in these cases:

- When you are **creating** a new Traditional VSX Gateway object for the **first time** for a Security Group.
- When you are **editing** an existing Traditional VSX Gateway object for a Security Group and changing the configuration of the Management interface (for example, `eth1-Mgmt1`).

You must manually set the state of all other Security Group Members to "Down", perform the required configuration in the Traditional VSX Gateway object, and then set the state of the Security Group Members to "Up":

1. Connect to the command line on the Security Group.
2. If your default shell is Gaia gClish, then go to the Expert mode:
   ```
   expert
   ```
3. Set all Security Group Members to the state "`DOWN`" (except for one Security Group Member):

   Best Practice - (missing or bad snippet)

   ```
   g_clusterXL_admin -b <ID of first selected SGM"> down
   g_clusterXL_admin -b <ID of second selected SGM"> down
   ...
   ```

   Example:

   ```
   [Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_2
   down
   [Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_3
   down
   [Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_4
   down
   ```
4. Examine the state of the Security Group Members:
   ```
   asg monitor
   ```
5. On the Management Server, perform the required configuration of the Traditional VSX Gateway object.
   The Management Server pushes the updated Traditional VSX configuration to the Security Group.
6. Install the applicable Access Control Policy on the Traditional VSX object.
   The Management Server creates this policy automatically when you create the Traditional VSX Gateway object.
7. On the Security Group, set the Security Group Members to the state "`UP`".
   ```
   g_clusterXL_admin -b <ID of first selected SGM"> up
   g_clusterXL_admin -b <ID of second selected SGM"> up
   ...
   ```
8. Examine the state of the Security Group Members:

```
asg monitor
```

Procedure:

1. **Configure the applicable Security Groups on the Maestro Orchestrators**

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

   Each Security Group must contain:

   a. One or more Security Appliances.

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

   b. Applicable ports on the 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 Maestro in Gaia Portal" on page 111*).
   - Gaia Clish (see *"Configuring Security Groups in Maestro in Gaia Clish" on page 124*).

   See *"Summary of Configuration Options in Maestro" on page 107*.

   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. **Note** - This First Time Wizard configures only a limited number of settings.

Step	Instructions
d	Assign the available Security Appliances to the Security Group. **Important:** ▪ You can assign only supported Security Appliances to the same Security Group - see sk162373. ▪ 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.
e	Assign the applicable Maestro Orchestrator ports to the Security Group (Uplink ports and a Management interface).

Best Practice - Create a Gaia Backup on the Maestro Orchestrators to save the configuration. For more information, see the *R82 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 in Maestro" on page 159*.

   Best Practice - Create a Gaia Backup on the Security Group to save the configuration. For more information, see the *R82 Gaia Administration Guide* > Chapter *Maintenance* > Section *System Backup*.

3. **Configure the settings in SmartConsole**

   See *"Step 3 - Configuration of a Maestro Security Group in SmartConsole" on page 161*.

   ▪ 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 in Maestro" on page 170*.

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 in Maestro" on page 173*
   - *"Configuring Security Group High Availability in Maestro" on page 255*
   - *"Managing Security Groups" on page 535*
   - *"System Optimization in Maestro" on page 217*
   - *"Deploying a Security Group in Monitor Mode" on page 578*
   - *"Deploying a Security Group in Bridge Mode" on page 615*

Step 1 - Configuration Procedure in Maestro

You can configure Security Groups on Maestro Orchestrators:

- In Gaia Portal (see *"Configuring Security Groups in Maestro in Gaia Portal" on page 111*)
- In Gaia Clish (see *"Configuring Security Groups in Maestro in Gaia Clish" on page 124*)

See *"Summary of Configuration Options in Maestro" on page 107*.

Workflow for Configuring Security Groups in Maestro

You can configure Security Groups on a Maestro Orchestrator:

- In Gaia Portal - see *"Configuring Security Groups in Maestro in Gaia Portal" on page 111*
- In Gaia Clish - see *"Configuring Security Groups in Maestro in Gaia Clish" on page 124*

See *"Summary of Configuration Options in Maestro" on page 107*.

Workflow:

Step	Instructions
1	Create a new Security Group. **Note** - Configure only one of the installed Maestro Orchestrators. The Maestro Orchestrators synchronize the configuration automatically with each other. **Important** - You must configure the **First Time Wizard settings** when you create a new Security Group.
2	Assign the applicable Security Appliances to the Security Group. **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.
3	Assign the applicable Maestro Orchestrator ports to the Security Group: ■ Uplink ports ■ A Management interface
4	Verify and apply the configuration.

Step	Instructions
5	If you did not configure the **First Time Wizard settings** when you created a Security Group, you must run the Gaia First Time Configuration Wizard on the Security Group. a. With a web browser, connect to the Gaia Portal of the Security Group: `https://<IP Address of Security Group>` **Important** - This connection goes through the Maestro Orchestrator's management interface you assigned to this Security Group. b. The Gaia First Time Configuration Wizard starts. Follow the instructions on the screen.

Summary of Configuration Options in Maestro

Table: Summary of configuration options in Maestro Orchestrators

Configuration Option	In Gaia Portal	In Gaia Clish*
Configuring the number of Maestro sites (Single Site or Dual Site)	N / A	See *"Configuring the Number of Maestro Sites" on page 126*
Viewing the configured number of Maestro sites	1. Click **Orchestrator** page. 2. In the **Topology** pane, open the Security Groups.	See *"Viewing the Number of Maestro Sites" on page 126*
Configuring the Site ID in the Dual Site deployment	N / A	See *"Configuring the Site ID in Dual Site Deployment" on page 127*
Viewing the Site ID in the Dual Site deployment	N / A	See *"Viewing the Site ID in Dual Site Deployment" on page 128*
Configuring the number of Orchestrators on a Maestro Site	N / A	See *"Configuring the Number of Orchestrators on a Maestro Site" on page 127*
Viewing the configured number of Orchestrators on a Maestro Site	N / A	See *"Viewing the Number of Orchestrators on a Maestro Site" on page 127*
Creating a New Security Group	See *"Creating a New Security Group" on page 113*	See *"Creating a New Security Group" on page 130*
Deleting a Security Group	See *"Deleting a Security Group" on page 114*	See *"Creating a New Security Group" on page 130*
Adding the Network Configuration to a Security Group	See *"Adding the Network Configuration and First Time Wizard settings to a Security Group" on page 115*	See *"Adding the Network Configuration to a Security Group" on page 132*
Removing the Network Configuration from a Security Group	See *"Removing the Network Configuration and First Time Wizard settings from a Security Group" on page 116*	See *"Removing the Network Configuration from a Security Group" on page 133*

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

Configuration Option	In Gaia Portal	In Gaia Clish*
Configuring the First Time Wizard settings in a Security Group	See *"Adding the Network Configuration and First Time Wizard settings to a Security Group" on page 115*	See *"Configuring First Time Wizard settings in a Security Group" on page 134*
Removing the First Time Wizard settings from a Security Group	See *"Removing the Network Configuration and First Time Wizard settings from a Security Group" on page 116*	See *"Removing First Time Wizard settings from a Security Group" on page 135*
Assigning available Security Appliances to a Security Group	See *"Assigning Available Security Appliances to a Security Group" on page 117*	See *"Assigning One Security Appliance to a Security Group" on page 136*
Removing one Security Appliance from a Security Group	See *"Removing One Security Appliance from a Security Group" on page 118*	See *"Removing One Security Appliance from a Security Group" on page 138*
Removing all Security Appliances from a Security Group	See *"Removing All Security Appliances from a Security Group" on page 119*	N / A
Moving Security Appliances from one Security Group to a different Security Group	See *"Moving Security Appliances from One Security Group to a Different Security Group" on page 120*	N / A
Assigning Interfaces to a Security Group	See *"Assigning Interfaces to a Security Group" on page 121*	See *"Assigning One Interface to a Security Group" on page 140*
Removing one interface from a Security Group	See *"Removing One Interface from a Security Group" on page 121*	See *"Removing One Interface from a Security Group" on page 141*
Removing all interfaces from a Security Group	See *"Removing All Interfaces from a Security Group" on page 122*	N / A
Moving interfaces from one Security Group to a different Security Group	See *"Moving Interfaces from One Security Group to a Different Security Group" on page 122*	N / A

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

Configuration Option	In Gaia Portal	In Gaia Clish*
Adding VLAN interfaces on Uplink ports	N / A	See *"Configuring VLAN Interfaces on Uplink Ports a Maestro Security Group" on page 195*
Viewing VLAN interfaces on Uplink ports	See *"Configuring VLAN Interfaces on Uplink Ports a Maestro Security Group" on page 195* Follow these steps: 1. Click **Orchestrator** page. 2. See the **Unassigned Interfaces** column. or these steps: 1. Click **Orchestrator** page. 2. Click the **[+]** on the left side of the applicable Security Group. 3. Click the **[+]** on the left side of the **Interfaces** section.	See *"Viewing VLAN Interfaces on Uplink Ports" on page 142* See *"Configuring VLAN Interfaces on Uplink Ports a Maestro Security Group" on page 195*
Verifying the configuration changes in Security Groups	Automatic	See *"Verifying the Configuration Changes" on page 143*
Applying the configuration changes to Security Groups	In the bottom left corner, click **Apply**.	See *"Applying the Configuration Changes" on page 144*
Deleting configuration changes in Security Groups that were not applied yet	In the bottom left corner, click **Refresh**.	See *"Deleting Configuration Changes That Were Not Applied Yet" on page 145*
Configuring the port settings	N / A	See *"Configuring the Port Settings" on page 146*
Viewing the port settings	N / A	See *"Viewing the Port Settings" on page 153*

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

Configuration Option	In Gaia Portal	In Gaia Clish*
Viewing the Security Group settings	Follow these steps: 1. Click **Orchestrator** page. 2. In the **Topology** column, click the **[+]** on the left side of the **Security Groups**. 3. Click the **[+]** on the left side of the applicable Security Group.	See *"Viewing the Security Group Settings" on page 157*

*Important - After every change in Gaia Clish, verify (see *"Verifying the Configuration Changes" on page 143*) and then apply (see *"Applying the Configuration Changes" on page 144*) the new configuration.

Configuring Security Groups in Maestro in Gaia Portal

This section provides the configuration instructions for Gaia Portal.

To start working in Gaia Portal on the Maestro Orchestrator:

Step	Instructions
1	With a web browser, connect to the Gaia Portal on the Maestro Orchestrator: `https://<IP Address of Orchestrator's MGMT Port>`
2	Log in to the Gaia Portal with these default credentials: ■ Username - `admin` ■ Password - `admin` **Best Practice** - Change the default password as soon as possible. See the *R82 Gaia Administration Guide* > Chapter *User Management* > Section *Change My Password*.
3	From the left navigation tree, in the **Orchestrator Management** section, click the **Security Groups** page.

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

Item	Description
Unassigned Gateways	All detected Security Appliances that are not part of configured Security Groups. Maestro Orchestrator listens on the ports and automatically detects the connected Security Appliances.
Topology	Configured Security Groups with their assigned Security Appliances and ports.
Unassigned Interfaces	All interfaces on 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 Maestro Orchestrators for redundancy, and you change the configuration on another 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 in Maestro" on page 105*.

Creating a New Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	In the **Topology** column, right-click on the **Security Groups** and select **New Security Group**.
3	Enter the required **Management interface settings**. **Important** - You must configure the **First Time Wizard settings** when you create a new Security Group.
4	Click **OK**.
5	Click the **[+]** on the left side of the **Security Groups** and the new Security Group.
6	In the **Unassigned Gateways** column, select the applicable Security Appliances. **Important** - You must assign at least one Security Appliance to the Security Group. **Notes:** ▪ 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). ▪ To select multiple Security Appliances, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
7	Drag-and-drop the selected Security Appliances from the **Unassigned Gateways** column to the **Gateways** section in the new Security Group.
8	In the **Unassigned Interfaces** column, select the applicable data and management interfaces. **Note** - To select multiple interfaces, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
9	Drag-and-drop the selected interfaces from the **Unassigned Interfaces** column to the **Interfaces** section in the new Security Group.
10	In the bottom left corner, click **Apply**. **Important** - 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 **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	In the **Topology** column, right-click on the Security Group.
3	From the menu, click **Delete Security Group**. **Important** - There is no prompt to confirm.
4	In the bottom left corner, click **Apply**.

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

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	In the **Topology** column, right-click on the Security Group.
3	Click **Set Security Group configuration**.
4	In the **Network settings** section: 1. In the **IPv4 address** 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. 2. In the **Subnet mask** 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. 3. In the **Default Gateway** field, enter the applicable IPv4 address. All Security Appliances in this Security Group use this IPv4 address as their default gateway.
5	In the **First Time Wizard settings** section, configure the initial settings for Security Appliances assigned to this Security Group. 1. Select **Set FTW configuration**. 2. In the **Host Name** field, enter a hostname. 3. Select **Configure Admin Password**: a. In the **Admin Password** field, enter the Expert mode password. b. In the **Confirm Admin Password** field, enter the same Expert mode password key again. 4. In the **SIC Password** 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. 5. In the **Confirm SIC Password** field, enter the same one-time activation key again. 6. Select **Install as VSX**, only if it is necessary to run all Security Appliances in this Security Group as VSX Gateways.
6	Click **OK**.
7	In the bottom left corner, click **Apply**.

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

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 cluster configuration image auto-clone state on
   show cluster configuration image auto-clone state
   ```

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

   ```
   set cluster configuration image auto-clone state off
   show cluster configuration image auto-clone state
   ```

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	In the **Unassigned Gateways** column, select the applicable Security Appliances. **Note** - To select multiple Security Appliances, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
4	Drag-and-drop the selected Security Appliances from the **Unassigned Gateways** column to the **Gateways** section in the applicable Security Group. **Note** - 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 **Apply**.

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 **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	Click the **[+]** on the left side of the **Gateways** 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 **Detach Gateway**. **Important** - There is no prompt to confirm.
7	In the bottom left corner, click **Apply**.

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

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 cluster configuration image auto-clone state on
   show cluster configuration image auto-clone state
   ```

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

   ```
   set cluster configuration image auto-clone state off
   show cluster configuration image auto-clone state
   ```

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable *source* Security Group.
3	Click the **[+]** on the left side of the applicable *target* Security Group.
4	Select the applicable Security Appliances. **Note** - To select multiple Security Appliances, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
5	Drag-and-drop the selected Security Appliances from the **Gateways** section of the *source* Security Group to the **Gateways** section of the *target* Security Group. **Note** - 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 **Apply**.

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.

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

Assigning Interfaces to a Security Group

Step	Instructions
1	In the **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable Security Group.
3	In the **Unassigned Interfaces** column, select the applicable interfaces. **Note** - To select multiple interfaces, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
4	Drag-and-drop the selected interfaces from the **Unassigned Interfaces** column to the **Interfaces** section in the applicable Security Group. **Note** - 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 **Apply**.

Removing One Interface from a Security Group

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

Removing All Interfaces from a Security Group

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

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 **Topology** column, click the **[+]** on the left side of the **Security Groups**.
2	Click the **[+]** on the left side of the applicable *source* Security Group.
3	Click the **[+]** on the left side of the applicable *target* Security Group.
4	Select the applicable interfaces. **Note** - To select multiple interfaces, press and hold the **CTRL** key and left-click the objects with the mouse cursor.
5	Drag-and-drop the selected interfaces from the **Interfaces** section of the *source* Security Group to the **Interfaces** section of the *target* Security Group. **Note** - 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 **Apply**.

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

Viewing VLAN Interfaces on Uplink Ports

See *"Configuring VLAN Interfaces on Uplink Ports a Maestro Security Group" on page 195*.

Step	Instructions
1	On the **Orchestrator** page, in the **Topology** section, expand **Security Groups**.
2	Expand your Security Group.
3	Expand **Interfaces**.
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 Maestro in Gaia Clish

This section provides the configuration instructions for Gaia Clish.

To start working in Gaia Clish on the Maestro Orchestrator:

Step	Instructions
1	Connect to the Command Line on the Maestro Orchestrator (over SSH, or through the Console Port).
2	Log in to the Gaia Portal with these default credentials: ■ Username - `admin` ■ Password - `admin` **Best Practice** - Change the default password as soon as possible. See the *R82 Gaia Administration Guide* > Chapter *User Management* > Section *Change My Password*.

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

Task	Syntax
Viewing the settings	`show maestro` **Available sub-commands** To see all available sub-commands: 1. Enter: `show maestro` 2. Press the **Esc** key two times.
Configuring the settings	`add maestro` **Available sub-commands** To see all available sub-commands: 1. Enter: `add maestro` 2. Press the **Esc** key two times.
	`set maestro` **Available sub-commands** To see all available sub-commands: 1. Enter: `set maestro` 2. Press the **Esc** key two times
Deleting the settings	`delete maestro` **Available sub-commands** To see all available sub-commands: 1. Enter: `delete maestro` 2. Press the **Esc** key two times

Notes:

- For more information about the Gaia Clish, see the *R82 Gaia Administration Guide*.
- After every change, verify (see *"Verifying the Configuration Changes" on page 143*) and then apply (see *"Applying the Configuration Changes" on page 144*) the new configuration.

Applicable configuration procedures are provided below.

See *"Workflow for Configuring Security Groups in Maestro" on page 105*.

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

The 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. Maestro Orchestrators of the same site use this value to calculate internal VLAN ID used for internal synchronization between Maestro Orchestrators.

Important:

- The value of the Base Site Sync VLAN ID must be the same on all 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.

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

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

  ```
  <Site Sync VLAN ID> = <Base Site Sync VLAN ID> + 0
  ```

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

  ```
  <Site Sync VLAN ID> = <Base Site Sync VLAN ID> + 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 security-appliances inter-site base-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 Maestro Orchestrator.

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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs and the available ID, press the **Tab** key. **Important** - The largest shown ID is the next available ID.

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 Maestro Orchestrator.

Important - There is no prompt to confirm.

Syntax

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

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** 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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`<Security Group IPv4 Address>`	Specifies the IPv4 address for the Security Group.
`<Default Gateway IPv4 Address>`	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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** 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.

Important - You must configure the **First Time Wizard settings** when you create a new 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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`ftw-configuration`	Specifies the First Time Wizard settings for Security Appliances in the Security Group.
`hostname <Hostname>`	Specifies the hostname for Security Appliances.
`sic <SIC Password>`	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.
`admin-password <Admin Password>`	Specifies the Expert mode password for the Security Group.
`is-vsx {yes | no}`	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
id <*Security Group ID*>	Specifies the Security Group ID. To see the existing IDs, press the **Tab** 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 cluster configuration image auto-clone state on
   ```

   ```
   show cluster configuration image auto-clone state
   ```

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

   ```
   set cluster configuration image auto-clone state off
   ```

   ```
   show cluster configuration image auto-clone state
   ```

Description

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

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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`serial <Serial Number>`	Assigns one Security Appliance specified by its Serial Number. To see the available Serial Numbers, press the **Tab** key. **Important** - 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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`member <Member ID>`	Specifies the Security Appliance by its Member ID in the Security Group. To see the available IDs, press the **Tab** key.
`serial <Serial Number>`	Specifies the Security Appliance by its Serial Number. To see the available Serial Numbers, press the **Tab** 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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`interface <Interface Name>`	Assigns one interface specified by its name. To see the available interfaces, press the **Tab** 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
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** key.
`interface <Interface Name>`	Removes one interface specified by its name. To see the available interfaces, press the **Tab** 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 a Maestro Security Group" on page 195*.

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
`id <Security Group ID>`	Specifies the ID of the Security Group. To see the existing IDs, press the **Tab** 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.

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 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
<Port ID>	Specifies the port to configure. The format is three numbers separated with a slash: *<Maestro Orchestrator ID>/<Port Label>/<Port Split ID>* Examples: ■ 1/3/1 ■ 2/20/1 Notes: ■ *<Maestro Orchestrator ID>* is 1 if you connect only one Maestro Orchestrator. When you connect two Maestro Orchestrators for redundancy, the *<Maestro Orchestrator ID>* is 1 on the first Maestro Orchestrator and 2 on the second Maestro Orchestrator. ■ *<Port Label>* is the number of the physical port on the front panel. On MHO-140, there are exceptions for ports 51, 53, 55, and 56. ■ The default value of the *<Port Split ID>* is 1, if you did not split the port with a breakout cable. ■ To see the available Port IDs, enter the command `set maestro port` and press the **Tab** key. ■ To see the Port IDs and the names Gaia OS assigned to them, connect to the Gaia Portal on the Maestro Orchestrator and click **Orchestrator** page. For the default mapping, see the *Maestro Getting Started Guide* - Section *Maestro Hyperscale Orchestrator Ports and Gaia OS Interfaces*.
`admin-state`	Configures the port administrative state: ■ `up` - Enabled ■ `down` - Disabled **Important** - This change does **not** survive reboot of the Orchestrator (Known Limitation MBS-11339).
`mtu`	Configures the port MTU. Valid range: 68 - 10236 bytes. Default: 10236 bytes.

Parameter	Description

`qsfp-mode`	Configures the QSFP mode:
	■ `1G` - Port works with the 1 GbE speed (only 10 GbE ports support this mode).
	■ `10G` - Port works with the 10 GbE speed.
	■ `4x10G` - Split of a 40 GbE port into four ports that work with the 10 GbE speed each.
	■ `4x25G` - Split of a 100 GbE port into four ports that work with the 25 GbE speed each.
	■ `25G` - Port works with the 25 GbE speed.
	■ `40G` - Port works with the 40 GbE speed.
	■ `100G` - Port works with the 100 GbE speed.
	Important
	■ On MHO-175 ports, you can configure only these modes:
	• `4x10G`, `4x25G`, `25G`, `40G`, or `100G`
	■ On MHO-170 ports, you can configure only these modes:
	• Ports with odd <*Port Label*> numbers (x/1/y, x/3/y, x/5/y, and so on):
	`4x10G`, `4x25G`, `25G`, `40G`, or `100G`
	• Ports with even <*Port Label*> numbers (x/2/y, x/4/y, x/6/y, and so on):
	`25G`, `40G`, or `100G`
	■ On MHO-140 ports, you can configure only these port modes:
	• Ports with the <*Port Label*> from x/1/y to x/48/y:
	`1G`, `10G`, or `25G`
	• Ports with the <*Port Label*> x/49/y, x/51/y, x/53/y, and x/55/y:
	`4x10G`, `4x25G`, `25G`, `40G`, or `100G`
	• Ports with the <*Port Label*> x/50/y, x/52/y, x/54/y, and x/56/y:
	`25G`, `40G`, or `100G`

Parameter	Description
`type`	Configures the port type: ■ `downlink` - Connects to Check Point Security Appliances ■ `uplink` - Connects to external and internal production networks ■ `management` - Connects to a Management Server that manages the applicable Security Group ■ `site_sync` - External synchronization in Dual Site deployment - between peer Orchestrators on different sites ■ `ssm_sync` - Internal synchronization in Dual Site deployment - between peer Orchestrators on the same site The parameter "`no-confirmation`" is optional. If specified, the command does not ask you for confirmation and audit information.

Parameter	Description
	Important: ■ On MHO-175, you can configure only these port types: • Port 1: ◦ `management` ◦ `downlink` • Ports 2 and higher: ◦ `uplink` ◦ `downlink` ◦ `site_sync` ◦ `ssm_sync` ■ On MHO-170, you can configure only these port types: • Port 1 and Port 2: ◦ `management` ◦ `downlink` • Ports 3 and higher: ◦ `uplink` ◦ `downlink` ◦ `site_sync` ◦ `ssm_sync` ■ On MHO-140, you can configure only these port types: • Port 1, Port 2, Port 3, and Port 4: ◦ `management` ◦ `downlink` • Ports 5 and higher: ◦ `uplink` ◦ `downlink` ◦ `site_sync` ◦ `ssm_sync` ■ You cannot change the "`ssm_sync`" type of the dedicated Internal Synchronization port: • MHO-175 - Port 32 • MHO-170 - Port 32 • MHO-140 - Port 48

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 Maestro Orchestrator's ports.

Syntax

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

Parameters

Parameter	Description
`<Port ID>`	Specifies the port to configure. The format is three numbers separated with a slash: `<Maestro Orchestrator ID>/<Port Label>/<Port Split ID>` Examples: ■ `1/3/1` ■ `2/6/1` Notes: ■ If the port is not split with a breakout cable, then the default value of the `<Port Split ID>` is 1. ■ To see the available Port IDs, press the **Tab** key. ■ To see the Port IDs and the names Gaia OS assigned to them, connect to the Gaia Portal on the Maestro Orchestrator and click **Orchestrator** page. For the default mapping, see the *Maestro Getting Started Guide* > Section *Maestro Orchestrator Ports and Gaia OS Interfaces*.
`admin-state`	Shows the port administrative state: ■ `up` - Enabled ■ `down` - Disabled
`mtu`	Shows the port MTU.
`optic-info`	Shows the information about the QSFP transceiver.
`qsfp-mode`	Shows the QSFP mode: ■ `1G` - Port works with the 1 GbE speed (only 10 GbE ports support this mode). ■ `10G` - Port works with the 10 GbE speed. ■ `4x10G` - Split of a 40 GbE port into four ports that work with the 10 GbE speed each. ■ `4x25G` - Split of a 100 GbE port into four ports that work with the 25 GbE speed each. ■ `25G` - Port works with the 25 GbE speed. ■ `40G` - Port works with the 40 GbE speed. ■ `100G` - Port works with the 100 GbE speed.

Parameter	Description
`type`	Shows the port type: ■ `uplink` - Connects to external and internal production networks ■ `downlink` - Connects to Check Point Security Appliances ■ `management` - Connects to a Management Server that manages the applicable Security Group ■ `site_sync` - External synchronization in Dual Site deployment - between peer Orchestrators on different sites ■ `ssm_sync` - Internal synchronization in Dual Site deployment - between peer Orchestrators on the same site
`vlans`	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 qsfp-mode
Port 27 qsfp-mode is 10G
MHO>
MHO> show maestro port 1/55/1 qsfp-mode
Port 55 qsfp-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 Maestro Orchestrator.

Syntax

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

Parameters

Parameter	Description
`id <Security Group ID>`	Specifies the Security Group ID. To see the existing IDs, press the **Tab** 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 Point 16000
  - 3:
   - serial: 3333333333
   - model: Check Point 16000
  - 2:
   - serial: 4444444444
   - model: Check Point 16000
  - 4:
   - serial: 5555555555
   - model: Check Point 16000
 - mgmt_netmask: 24
MHO>
```

Step 2 - Configuring Gaia Settings of a Security Group in Maestro

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	With a web browser, connect to the Gaia Portal of the Security Group: `https://<IP Address of Security Group>` **Important** - This connection goes through the Maestro Orchestrator's management interface you assigned to this Security Group.
2	Log in with these default credentials: ■ Username - `admin` ■ Password - `admin`
3	Change the default Gaia password to a new password: a. From the left tree, click **User Management > Users**. b. Select the **admin** user. c. Click **Reset Password**. d. Enter the new password. e. Click **OK**.
4	From the left tree, click **Network Management > Network Interfaces**.
5	Configure the applicable settings (for example, create a Bond or a VLAN interface) and IP addresses for the Uplink ports. **Important** - In VSX mode, you must configure all IP addresses in SmartConsole only. **Note** - Maestro Security Groups do not support an IPv6 address on eth<X>-Mgmt<X> interfaces (Known Limitation MBS-5482)
6	Configure other applicable Gaia settings. For example: Time Zone, DNS servers, Proxy server, Static Routes.

For more information, see the *R82 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	Connect to the command line of the Security Group over SSH at *<IP Address of Security Group>*. When you log in, the Gaia gClish opens by default. **Important** - This connection goes through the Maestro Orchestrator's management interface you assigned to this Security Group.
2	Log in with these default credentials: ■ Username - `admin` ■ Password - `admin`
3	Change the default Gaia password to a new password: `set user admin password`
4	Configure the applicable settings (for example, create a Bond or a VLAN interface) and IP addresses for the Uplink ports. **Important** - In VSX mode, you must configure all IP addresses in SmartConsole only. **Note** - Maestro Security Groups do not support an IPv6 address on eth<X>-Mgmt<X> interfaces (Known Limitation MBS-5482).
5	Configure other applicable Gaia settings. For example: Time Zone, DNS servers, Proxy server, Static Routes.

For more information, see:

- *R82 Gaia Administration Guide*
- *"Connecting to a Specific Security Group Member in Maestro" on page 206*

Step 3 - Configuration of a Maestro Security Group 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 **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click **New (✳) > Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter a name for this Security Gateway object. b. In the **Gateway platform** field, select **Maestro**. c. In the **Gateway IP address** section, enter the same IPv4 address that you configured for the Security Group on the Maestro Orchestrator. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select **Initiate trusted communication now**, enter the same Activation Key you entered in the **First Time Wizard settings** of the Security Group on the Maestro Orchestrator. b. Click **Next**.

Step	Instructions
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.
8	On the **Network Security** tab, enable the desired Software Blades. **Important** - Do **not** select anything on the **Management** tab.
9	Click **OK**.
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 **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click **New (✳) > Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > Gateway**.
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter a name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, enter the same IPv4 address that you configured for the Security Group on the Maestro Orchestrator.

Step	Instructions
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field, select **Open server / Appliance**. c. In the **Activation Key** field, enter the same Activation Key you entered in the **First Time Wizard settings** of the Security Group on the Maestro Orchestrator. d. Click **Initialize**. e. Click **OK**.
8	In the **Platform** section, select the correct options: a. In the **Hardware** field, select **Maestro**. b. In the **Version** field, select **R80.20SP**. c. In the **OS** field, select **Gaia**.
9	On the **Network Security** tab, enable the desired Software Blades. **Important** - Do **not** select anything on the **Management** tab.
10	Click **OK**.
11	Publish the SmartConsole session.

For more information, see the *R82 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 **Security Policies**.

Step	Instructions
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.
4	Create the applicable Access Control Policy.
6	Create the applicable Threat Prevention Policy.
7	Publish the SmartConsole session.

For more information, see:

- *R82 Security Management Administration Guide*
- *R82 Threat Prevention Administration Guide*
- Applicable *Administration Guides* on the R82 Home Page.

3. **Install the Security Policy in SmartConsole**

Step	Instructions
1	Install the Access Control Policy on the Security Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for this Security Gateway object. c. Select only the Access Control Policy. d. Click **Install**.
2	Install the Threat Prevention Policy on the Security Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for this Security Gateway object. c. Select only the Threat Prevention Policy. d. Click **Install**.

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 *Main* Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new VSX Gateway object in one of these ways: ■ From the top toolbar, click **New (✦) > VSX > Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Gateway**. The **VSX Gateway Wizard** opens.
4	On the **VSX Gateway General Properties (Specify the object's basic settings)** page: a. In the **Enter the VSX Gateway Name** field, enter the desired name for this VSX Gateway object. b. In the **Enter the VSX Gateway IPv4** field, enter the same IPv4 address that you configured on the **Management Connection** page of the VSX Gateway's First Time Configuration Wizard. c. In the **Enter the VSX Gateway IPv6** field, enter the same IPv6 address that you configured on the **Management Connection** page of the VSX Gateway's First Time Configuration Wizard. d. In the **Select the VSX Gateway Version** field, select **R80.20SP**. e. Click **Next**.
5	On the **Virtual Systems Creation Templates (Select the Creation Template most suitable for your VSX deployment)** page: a. Select the applicable template. b. Click **Next**.

Step	Instructions
6	On the **VSX Gateway General Properties (Secure Internal Communication)** page: a. In the **Activation Key** field, enter the same Activation Key you entered in the **First Time Wizard settings** of the Security Group on the Maestro Orchestrator. b. In the **Confirm Activation Key** field, enter the same Activation Key again. c. Click **Initialize**. d. Click **Next**.
7	On the **VSX Gateway Interfaces (Physical Interfaces Usage)** page: a. Examine the list of the interfaces - it must show all the Uplink ports you assigned to this Security Group. b. If you plan to connect more than one Virtual System directly to the same Uplink port, you must select **VLAN Trunk** for that physical Uplink port. c. Click **Next**.
8	On the **Virtual Network Device Configuration (Specify the object's basic settings)** page: a. You can select **Create a Virtual Network Device** and configure the first desired Virtual System at this time (we recommend to do this later). b. Click **Next**.
9	On the **VSX Gateway Management (Specify the management access rules)** page: a. Examine the default access rules. b. Select the applicable default access rules. c. Configure the applicable source objects, if needed. d. Click **Next**. **Important** - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.
10	On the **VSX Gateway Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.

Step	Instructions
11	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
12	Open the VSX Gateway object.
13	On the **General Properties** page, click the **Network Security** tab.
14	Enable the desired Software Blades for the VSX Gateway object itself (context of VS0). Refer to: ■ sk79700: VSX supported features ■ sk106496: Software Blades updates - FAQ ■ Applicable *Administration Guides* on the R82 Home Page
15	Click **OK** to push the updated VSX Configuration. Click **View Report** for more information.
16	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
17	Install policy on the VSX Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the default policy for this VSX Gateway object. This policy is called: `<Name of VSX Gateway object>_VSX` c. Click **Install**.
18	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

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

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server, or each *Target* 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: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for the Virtual System object. c. Select only the Access Control Policy. d. Click **Install**.
8	Install the Threat Prevention Policy on these Virtual Systems: a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for the Virtual System object. c. Select only the Threat Prevention Policy. d. Click **Install**.
9	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

For more information, see:

- *R82 Security Management Administration Guide*
- *R82 VSX Administration Guide*
- Applicable *Administration Guides* on the R82 Home Page

Step 4 - License Installation in Maestro

Notes:

- Maestro Orchestrators do not require a license.
- On the Management Server, each Security Group is one Security Gateway object.
  Therefore, each Security Group consumes a Management license of one Security Gateway.
- Installing or removing a license is supported only on the SMO Security Group Member.
- For each Security Appliance, you must generate a Security Gateway license.
- You can install the licenses on the SMO Security Group Member before or after you add other Security Group Members to the Security Group.
  The Security Group keeps the installed licenses in a "license bank".
- When you add a new Security Group Member with a MAC address that matches one of the installed licenses on this Security Group, the new Security Group Member receives the correct license immediately.
- When you remove a Security Group Member from a Security Group, the Security Group keeps the corresponding license in a "license bank".
- To install a license with the `cplic put` command, before you run the Gaia First Time Configuration Wizard, you must run the `cplic put` command in the Expert mode.

Adding Licenses

1. Get the MAC address of the **Management** port on each Security Appliance.

   If you already added a Security Appliance to the Security Group

   a. Connect to the command line on the Security Group.

   b. Get the MAC address of the **eth1-Mgmt1** interface.

      Run the command in **one** of the shells:

      - In Gaia gClish, run:

        ```
        show interface eth1-Mgmt1 mac-addr
        ```

      - In the Expert mode mode, run:

        ```
        g_all ifconfig eth1-Mgmt1 | grep HWaddr
        ```

      Make sure you copy the MAC address of the correct Security Appliance.

If you did not add a Security Appliance to the Security Group yet

a. Connect to the command line on the Security Appliance.

b. Get the MAC address of the **Mgmt** interface.

Run the command in **one** of the shells:

- In Gaia Clish, run:

```
show interface Mgmt mac-addr
```

- In the Expert mode mode, run:

```
ifconfig Mgmt | grep HWaddr
```

2. Log in to *Check Point User Center*.
3. Generate a new **Security Gateway** license for each Security Appliance:
   a. For an IP address, enter the IP address of the Security Group that you assigned to in on the Orchestrator.

      All Security Group Members in the Security Group have the same Management IP address.

   b. For a MAC address, enter the MAC address of the **Management** port on the Security Appliance.

      Each Security Group Member must have a license generated for its MAC address.

   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.
4. Attach the licenses on the SMO Security Group Member:
   a. Connect to the command line on the Security Group.

   b. Run the required command in **one** of the shells:

   - In Gaia gClish, run:

```
cplic put <License String>
```

   - In the Expert mode mode, run:

```
g_all cplic put <License String>
```

Removing Licenses from a Specific Security Group Member

1. Connect to the command line on the Security Group.
2. Get the license signature (and copy it) in **one** of the shells:
   - In Gaia gClish, run:

     ```
     cplic [-b <ID of Security Group Member>] print -x
     ```

     Example for Security Group 1 and Security Group Member 2:

     ```
     cplic -b 1_02 print -x
     ```

   - In the Expert mode mode, run:

     ```
     g_all cplic [-b <ID of Security Group Member>] print -x
     ```

3. Remove the license from this Security Group Member in **one** of the shells:

   Note - This command works only on the SMO Security Group Member.

   - In Gaia gClish, run:

     ```
     cplic del <License Signature>
     ```

   - In the Expert mode mode, run:

     ```
     g_all cplic del <License Signature>
     ```

Notes:
- Error messages can appear about deleting licenses that do not exist. These errors come from other Security Group Members.
- This procedure removes the license from the "license bank" on the Security Group.

Step 5 - Special Configuration Scenarios in Maestro

This section contains special configuration scenarios:

- Weights for Security Group Members when different models of Security Appliances are assigned to the same Security Group

  See *"Configuring Weights for Security Group Members in Maestro" on page 174*.

- Bond interfaces

  See:

  - *"Configuring Bond Interface on the Management Ports of a Maestro Security Group" on page 179*.
  - *"Configuring Bond Interface on Uplink Ports of a Maestro Security Group" on page 183*.

- VLAN interfaces

  See:

  - *"Configuring VLAN Interfaces on top of a Bond Interface on Uplink Ports of a Maestro Security Group" on page 186*.
  - *"Configuring VLAN Interfaces on Uplink Ports a Maestro Security Group" on page 195*.

- Shared Uplink Ports

  See *"Shared Uplink Ports on a Maestro Security Group" on page 200*.

Configuring Weights for Security Group Members in Maestro

Note - Do **not** confuse this section with *"Configuring Security Group High Availability in Maestro" on page 255* 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 cluster configuration image auto-clone state off
show cluster configuration image auto-clone state
```

Calculating the Security Group Member Weight

Default Weight for each Security Group Member:

```
    Number of CPU Cores on this Security Group Member
------------------------------------------------------ x 100%
 Total Number of CPU Cores on all Security Group Members
```

Custom Weight for a Security Group Member:

```
    Local Weight of this Security Group Member
------------------------------------------------ x 100%
 Sum of all Weights of all Security Group Members
```

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 the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`
3	Configure the required weight: `set smo security-group sgm-weight id <SGM IDs> weight {default | 0-512}`
4	Apply the new configuration: `set smo security-group sgm-weight apply` **Important** - As a result of the calculation, some connections might move between the Security Group Members.

Parameters:

Parameter	Description
`sgm-weight id <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`weight {default | 0-512}`	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 the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`
3	Examine the weights: `show smo security-group sgm-weight <SGM IDs>` Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

Example 1:

```
[Global] SG-s01-01> show smo security-group sgm-weight all
SGM weights are:
1_01: 8 (33.33%)
1_02: 16 (66.67%)
[Global] SG-s01-01>
```

Example 2:

```
[Global] SG-s01-01> show smo security-group sgm-weight 1_2
SGM 1_2 weight is: 16 (66.67%)
[Global] SG-s01-01>
```

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 of a Maestro Security Group

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

1. In Gaia gClish, temporarily disable the Traditional VSX mode:
   ```
   set vsx off
   ```
2. Configure a Bond Interface on the Management Ports as described below.
3. In Gaia gClish, enable the Traditional 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 Maestro in Gaia Portal" on page 111*), or Gaia Clish (see *"Configuring Security Groups in Maestro in Gaia Clish" on page 124*).

Step	Instructions
1	Connect to one of the Maestro Orchestrators.
2	Create a new Security Group: a. In the **Network settings** section, enter a dummy IP address configuration. b. Configure the **First Time Wizard settings**.
3	Assign two available management interfaces `eth`*M*`-Mgmt`*X* and `eth`*N*`-Mgmt`*Y* 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: `gclish`
9	Check which `eth#-Mgmt#` interface has the IP address you assigned to the Security Group. In our example, we assume it is `eth`*M*`-Mgmt`*X*.

Step	Instructions
10	Add a new Bonding group with this syntax: `add bonding group <Bond ID> mgmt`
11	Add the free `ethN-MgmtY` interface (without an IP address) to the bonding group with this syntax: `add bonding group <Bond ID> mgmt interface ethN-MgmtY`
12	Assign the real IP address (you wish to use for this Security Group) to the Bonding group with this syntax: `set interface magg<Bond ID> ipv4-address <Real IPv4 Address> mask-length <Mask Length>`
13	Set the Bonding group as the new Gaia Management Interface: `set management interface magg<Bond ID>`
14	Delete the dummy IP address from the `ethM-MgmtX` interface: `delete interface ethM-MgmtX ipv4-address`
15	Add the free `ethM-MgmtX` interface (without an IP address) to the bonding group with this syntax: `add bonding group <Bond ID> mgmt interface ethM-MgmtX`
16	Connect to one of the 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 Maestro Orchestrators.

Step	Instructions
2	Assign a second available management interface `eth`*N*`-Mgmt`*Y* to the Security Group. You can perform this step in Gaia Portal (see *"Configuring Security Groups in Maestro in Gaia Portal" on page 111*), or Gaia Clish (see *"Configuring Security Groups in Maestro in Gaia Clish" on page 124*). In our example, we assume that the interface `eth`*M*`-Mgmt`*X* is already assigned.
3	Connect through the console port to the Security Appliance with Member ID 1 in this Security Group.
4	Log in to the Expert mode.
5	Go to the Gaia gClish: `gclish`
6	Change the IP address on the `eth`*M*`-Mgmt`*X* interface to some dummy IP address: `set interface eth`*M*`-Mgmt`*X* `ipv4-address <`*Dummy IPv4 Address*`> mask-length <`*Mask Length*`>`
7	Add a new Bonding group with this syntax: `add bonding group <`*Bond ID*`> mgmt`
8	Add the free `eth`*N*`-Mgmt`*Y* interface (without an IP address) to the bonding group with this syntax: `add bonding group <`*Bond ID*`> mgmt interface eth`*N*`-Mgmt`*Y*
9	Assign the real IP address to the Bonding group with this syntax: `set interface magg<`*Bond ID*`> ipv4-address <`*Real IPv4 Address*`> mask-length <`*Mask Length*`>`
10	Set the Bonding group as the new Gaia Management Interface: `set management interface magg<`*Bond ID*`>`
11	Delete the dummy IP address from the `eth`*M*`-Mgmt`*X* interface: `delete interface eth`*M*`-Mgmt`*X* `ipv4-address`

Step	Instructions
12	Add the free `ethM-MgmtX` interface (without an IP address) to the bonding group with this syntax: `add bonding group <Bond ID> mgmt interface ethM-MgmtX`
13	Connect to one of the Maestro Orchestrators.
14	Make sure the Security Group settings are correct.

15	On the Management Server, update the topology of interfaces in the corresponding Security Gateway object.
	If this Security Group is configured in the Gateway mode of VSNext mode:
	a. From the left navigation panel, click **Gateways & Servers**.
	b. Open the Security Gateway object.
	c. From the left tree, click **Network Management**.
	d. Click **Get Interfaces** > **Get Interfaces With Topology**.
	e. Examine the configuration and accept it.
	f. Click **OK**.
	g. Install the applicable Access Control Policy.
	If this Security Group is configured in the Traditional VSX mode:
	a. Connect to the command line on the Management Server.
	b. On a Multi-Domain Security Management Server, go to the context of the applicable Domain Management Server:
	`mdsenv <IP Address or Name of Domain Management Server>`
	c. Run this command and follow the instructions on the screen:
	`vsx_util change_interfaces`
	For infromation about this command, see the *R82 VSX Administration Guide*.

Configuring Bond Interface on Uplink Ports of a Maestro Security Group

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

   You perform this step on one of the Maestro Orchestrators.

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

   In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal on one of the Maestro Orchestrators.
2	Assign the applicable Uplink ports to the applicable Security Group. See *"Assigning Interfaces to a Security Group" on page 121*.
3	In the bottom left corner, click **Apply**.

   In Gaia Clish

Step	Instructions
1	Connect to the command line on one of the Maestro Orchestrators.
2	Log in to the Gaia Clish.
3	Assign the applicable Uplink ports to the applicable Security Group. See *"Assigning One Interface to a Security Group" on page 140*.
4	Verify the new configuration. See *"Verifying the Configuration Changes" on page 143*.
5	Apply the new configuration. See *"Applying the Configuration Changes" on page 144*.

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.

Step	Instructions
2	Configure the Bond interface on top of the Uplink ports.
3	In Gateway mode only: Assign the IP address to this Bond interface. **Important** - 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: `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. **Important** - 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 *R82 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 **Gateways & Servers**.
3	Open the applicable Security Gateway object.
4	From the left tree, click **Network Management**.
5	Click **Get Interfaces > Get Interfaces Without Topology**.
6	Click **OK**.
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 **Gateways & Servers**.
3	Open the applicable VSX Gateway object.
4	From the left tree, click **Physical Interfaces**.
5	Click **Add**.
6	Add the new interface. **Important** - Enter the same name (case sensitive) you see in the Gaia settings of this Security Group.
7	Click **OK**.
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 *R82 VSX Administration Guide*.

Configuring VLAN Interfaces on top of a Bond Interface on Uplink Ports of a Maestro Security Group

In This Section:

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 Maestro Orchestrator.

   In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal on one of the Maestro Orchestrators.
2	Add VLAN tags on the applicable Uplink Ports. See *"Configuring Security Groups in Maestro in Gaia Portal" on page 111*.
3	Assign the applicable Uplink ports with VLAN tags to the applicable Security Group. See *"Assigning Interfaces to a Security Group" on page 121*.
4	In the bottom left corner, click **Apply**.

   In Gaia Clish

Step	Instructions
1	Connect to the command line on one of the Maestro Orchestrators.
2	Log in to the Gaia Clish.
3	Add VLAN tags on the applicable Uplink Ports. See *"Configuring Security Groups in Maestro in Gaia Clish" on page 124*.

Step	Instructions
4	Assign the applicable Uplink ports to the applicable Security Group. See *"Assigning One Interface to a Security Group" on page 140*.
5	Verify the new configuration. See *"Verifying the Configuration Changes" on page 143*.
6	Apply the new configuration. See *"Applying the Configuration Changes" on page 144*.

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 Maestro Orchestrator.
4	In Gateway mode only: Assign the IP addresses to these VLAN interfaces. **Important** - 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.
3	Go to the Gaia gClish: `gclish`
4	Configure the Bond interface on top of the Uplink ports.

Step	Instructions
5	Add the same VLAN interfaces on the Bond interface, which you added in the Maestro Orchestrator.
6	In Gateway mode only: Assign the IP addresses to these VLAN interfaces. **Important** - 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 *R82 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 **Gateways & Servers**.
3	Open the applicable Security Gateway object.
4	From the left tree, click **Network Management**.
5	Click **Get Interfaces > Get Interfaces Without Topology**.
6	Click **OK**.
7	Install the Access Control Policy on this Security Gateway object.

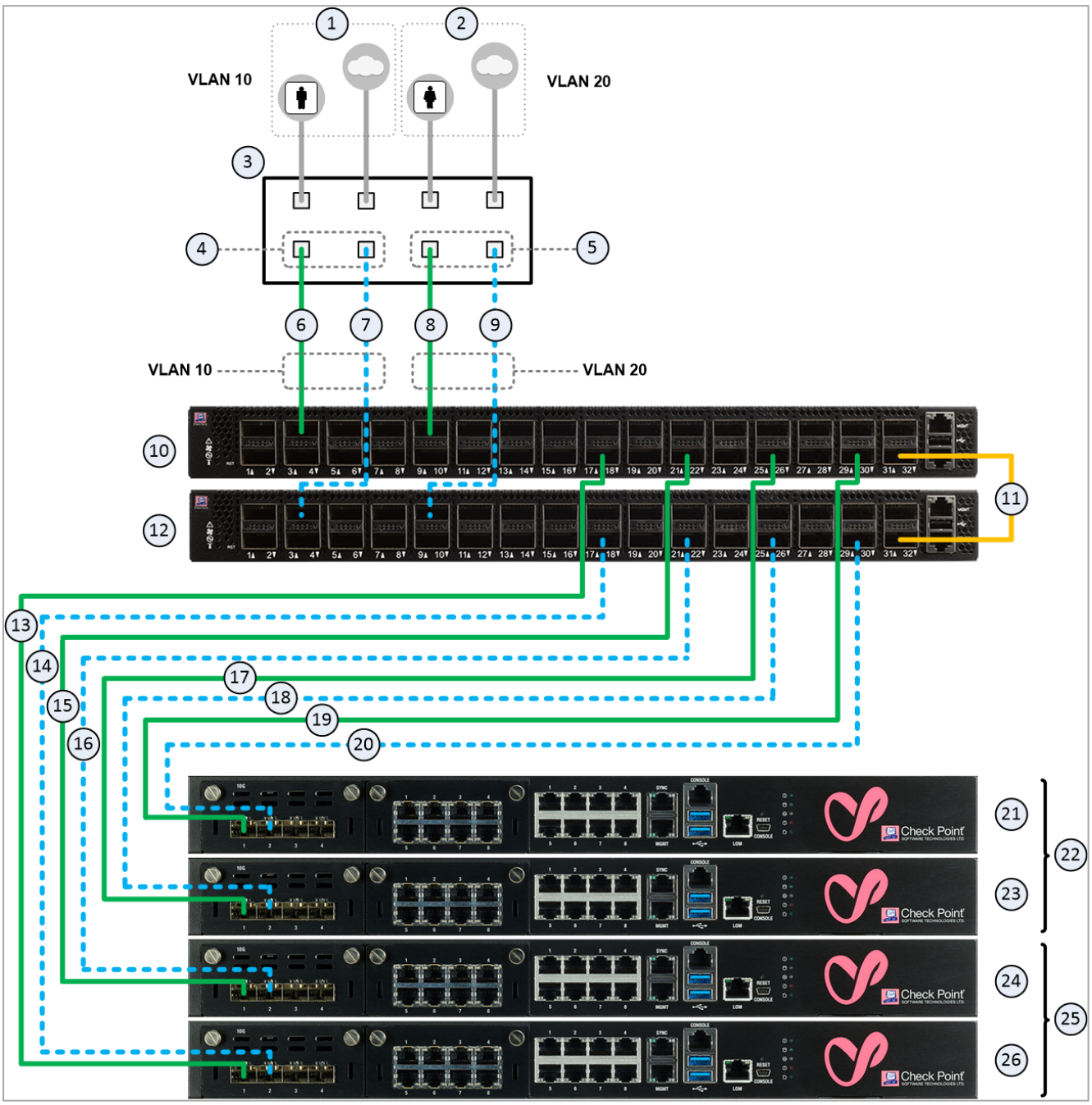
- If you already created a **VSX Gateway** object for this Security Group:

  Note - For more information, see the *R82 VSX Administration Guide*.

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the applicable VSX Gateway object.
4	From the left tree, click **Physical Interfaces**.
5	Click **Add**.
6	Add the new Bond interface. **Important** - Enter the same name (case sensitive) you see in the Gaia settings of this Security Group.
7	In the **VLAN Trunk** column, check the box for this Bond interface.
8	Click **OK**.
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 Maestro Orchestrators (**10** and **12**) with Bond interfaces (Link Aggregation).
4	Bond interface that connects Network 1 to the 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 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 Maestro Orchestrator (**10**). This cable connects to the Uplink port 3 (interface `eth1-05`), 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 Maestro Orchestrator (**12**). This cable connects to the Uplink port 3 (interface `eth2-05`), 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 Maestro Orchestrator (**10**). This cable connects to the Uplink port 9 (interface `eth1-17`), which must be configured with the VLAN tag 20.

Table: Explanations (continued)

Item	Description
9	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 Maestro Orchestrator (**12**). This cable connects to the Uplink port 9 (interface `eth2-17`), which must be configured with the VLAN tag 20.
10	First Maestro Orchestrator.
11	A DAC that connects the dedicated Synchronization ports 32 on the Maestro Orchestrators (**10** and **12**). **Important** - This connection is only used to synchronize the configuration of Security Groups between the Maestro Orchestrators.
12	Second Maestro Orchestrator.
13-20	DAC cables, Fiber cables (with transceivers), or Breakout cables that connect Downlink ports on 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	Configure the required settings on one of the Maestro Orchestrators: 1. Connect to one of the Maestro Orchestrators. 2. Add VLAN tag 10 to the Port 1/3/1 (interface `eth1-05`). 3. Add VLAN tag 10 to the Port 2/3/1 (interface `eth2-05`). 4. Add VLAN tag 20 to the Port 1/9/1 (interface `eth1-17`). 5. Add VLAN tag 20 to the Port 2/9/1 (interface `eth2-17`). 6. Assign the Port 1/3/1 with VLAN tag 10 (interface `eth1-05.10`) to the Security Group 1. 7. Assign the Port 2/3/1 with VLAN tag 10 (interface `eth2-05.10`) to the Security Group 1. 8. Assign the Port 1/9/1 with VLAN tag 20 (interface `eth1-17.20`) to the Security Group 2. 9. Assign the Port 2/9/1 with VLAN tag 20 (interface `eth1-17.20`) to the Security Group 2. 10. Apply the configuration.
2	Configure the required settings in the Security Group 1: 1. Connect to the Gaia of the Security Group 1. 2. Configure a new interface Bond1 on top of the interfaces `eth1-05` and `eth2-05`. 3. Add the VLAN tag 10 on top of the new interface Bond1 (`bond1.10`).
3	Configure the required settings in the Security Group 2: 1. Connect to the Gaia of the Security Group 2. 2. Configure a new interface Bond1 on top of the interfaces `eth1-17` and `eth2-17`. 3. Add the VLAN tag 20 on top of the new interface Bond1 (`bond1.20`).
4	In SmartConsole, add the new interface (`bond1.XX`) to the Security Group object.

Configuring VLAN Interfaces on Uplink Ports a Maestro Security Group

Introduction

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

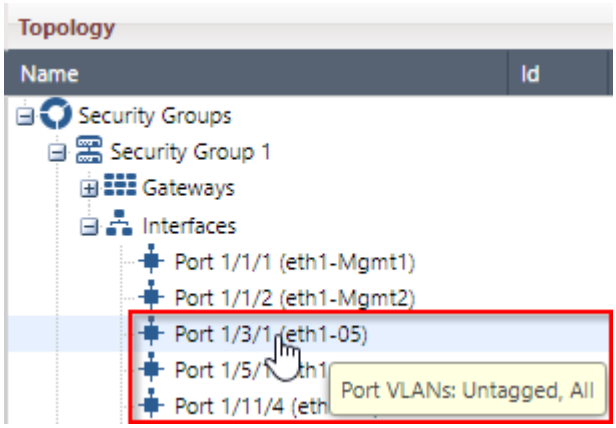
  If there are changes in the configuration of the Security Group interfaces (for example, VLAN interfaces or distribution mode), then the Security Group automatically sends these changes to the Orchestrator. The Security Group does so after a policy installation or a manual change in Gaia gClish.

Viewing VLAN Interfaces on Uplink Ports in Gaia Portal

Step	Instructions
1	On the **Orchestrator** page, in the **Topology** section, expand **Security Groups**.
2	Expand your Security Group.
3	Expand **Interfaces**.
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)

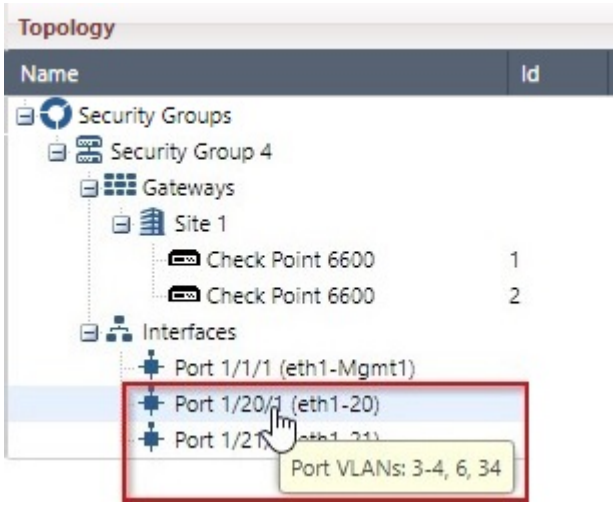
Tooltip:

- 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
`id <Security Group ID>`	Specifies the ID of the Security Group. To see the existing IDs, press the **Tab** 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	Enable the VLAN Trunk mode: `set maestro configuration uplink-trunk-mode state enabled`
4	Examine the status of the VLAN Trunk mode: `show maestro configuration uplink-trunk-mode state`
5	Restart the Maestro daemon: a. Connect to the command line on **each** Orchestrator on your sites. b. Log in to the Expert mode. c. Restart the 'orchd' process: `orchd restart`

Shared Uplink Ports on a Maestro Security Group

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. R82 must be installed on the Management Server.
2. R82 must be installed on the Maestro Orchestrators.
3. R82 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. Afterward, the subordinate interfaces in the bond must be added to each Security Group through the Maestro 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 Orchestrator:
   a. Enable the shared uplinks feature on Security Group 3 and Security Group 4:

   ```
   MHO_1_1> set maestro security-group id 3 shared-uplinks
   state enabled
   MHO_1_1> set maestro security-group id 4 shared-uplinks
   state enabled
   ```

   b. Apply the configuration:

   ```
   MHO_1_1> set maestro security-group apply-new-config
   ```

2. On the Maestro 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 (`/bin/bash`), 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-s01-01 > add bonding group 1 interface eth1-
05
[Global] sg3-s01-01 > add bonding group 1 interface eth2-
05
[Global] sg3-s01-01 > set bonding group 1 mode 8023AD
```

In Security Group 4, run:

```
[Global] sg4-s01-01 > add bonding group 1 interface eth1-
05
[Global] sg4-s01-01 > add bonding group 1 interface eth2-
05
[Global] sg4-s01-01 > set bonding group 1 mode 8023AD
```

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

In Security Group 3, run:

```
[Global] sg3-s01-01 > add interface bond1 vlan 30
```

In Security Group 4, run:

```
[Global] sg4-s01-01 > 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 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. If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish:

   ```
   gclish
   ```

   d. Remove the VLAN 40 interface from `bond1`.

   ```
   [Global] sg4-s01-01 > delete interface bond1 vlan 40
   ```

   e. Remove the subordinate interfaces `eth1-05` and `eth2-05` from `bond1`:

   ```
   [Global] sg4-s01-01 > delete bonding group 1 interface
   eth1-05
   [Global] sg4-s01-01 > delete bonding group 1 interface
   eth2-05
   ```

   f. Remove `bond1`:

   ```
   [Global] sg4-s01-01 > delete bonding group 1
   ```

2. On the Maestro 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 in Maestro

This section provides basic information about managing Security Groups in Maestro.

Connecting to a Specific Security Group Member in Maestro

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

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

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

2	Examine the configured Security Group and its Security Group Members with **one** of these commands.
	■ In Gaia Clish, run:
	`show maestro security-group id <Security Group ID>`
	You can press the Tab key to select the applicable Security Group ID.
	■ In the Expert mode, run:
	`clish -c "show maestro security-group id <Security Group ID>"`
	You must specify the required Security Group ID in the syntax.
	■ In the Expert mode, run:
	`orch_stat -t`
	See *"orch_stat" on page 1017*.

3	Connect to a Security Group Member in the Security Group with **one** of these commands:
	`member <Security Group ID> <Member ID>`
	`m <Security Group ID> <Member ID>`
	See *"member" on page 909*.

4	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-s01-03:0]#
```

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: `<IP Address of Security Group>` **Important** - This connection goes through the Maestro Orchestrator management interface you assigned to this Security Group.
2	Log in to Gaia gClish or the Expert mode.

3	Connect to a Security Group Member in the same Security Group with **one** of these commands:
	`member <Member ID>`
	`m <Member ID>`
	See *"member" on page 909*.

Example:

```
[Expert@SG1-s01-03:0]# 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-s01-02:0]#
```

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 Maestro Orchestrator or from another Security Group Member, the new SSH connection goes over an internal Maestro Orchestrator network.

Configuring a Unique IP Address per Site (UIPS) in Maestro Dual Site

In a Maestro Dual Site deployment:

- A heavy load on the Active Site can prevent you from creating a network connection to the SMO and working with management tasks.
- It can be necessary to have a direct access to the Standby Site to troubleshoot a problem, such as a Security Group Member in the DOWN state.

  You cannot use the SMO to connect to the Standby Site.

You can assign a unique IP address to each Standby Site to help resolve these issues.

This adds an alias IP address to the **management interface** that is assigned to the Security Group.

When there is a high load on the SMO, connect to the Standby Site using the unique IP address you assigned to the Standby Site.

The Security Group Members on the Standby Site are always in the state "`UP`" and available to run Gaia gClish commands.

Notes:

- The UIPS feature is disabled by default in Maestro.
- The UIPS feature does not support IPv6 addresses (Known Limitation MBS-9128).
- The UIPS feature in Maestro supports only the management interface that is assigned to a Security Group.
- Only one Security Group Member runs the "UIPS" task (similar to the "SMO" task).
  In the CLI output, this task appears as "UIPC" (the former name of this feature is "Unique IP Address per Chassis").

Description

Use the "`set cluster configuration unique-ip ...`" command in Gaia gClish to assign a unique IP address to a Standby Site.

Important - After you assign a unique IPv4 address to a Standby Site, you must make sure the Access Control policy of the Security Group allows the connection to the alias IP address.

Syntax

- *"show cluster configuration unique-ip" on page 965*
- *"set cluster configuration unique-ip" on page 931*

`show cluster configuration unique-ip site-id <ID of Standby Site> interface <Name of Mgmt Interface>`
`set cluster configuration unique-ip <ID of Standby Site> interface <Name of Mgmt Interface> ipv4-address <IPv4 Address> mask-length <Length of Subnet Mask>`
`set cluster configuration unique-ip <ID of Standby Site> apply_unique_config`
`delete cluster configuration unique-ip site-id <ID of Standby Site> interface <Name of Mgmt Interface>`

Parameters

Parameter	Description
<ID of Standby Site>	Specifies the ID of the Standby Site. Valid values: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
<Name of Mgmt Interface>	Specifies the name of the Management Interface that is assigned to the Security Group. For example, `eth1-Mgmt1`.
<IPv4 Address>	Specifies the alias IPv4 address on the same network as one of the Security Group Members' interfaces.
<Length of Subnet Mask>	Specifies the length of the IPv4 subnet mask.

Example 1 - Adding a UIPS

```
[Expert@HostName-s01-01:0]# gclish
[Global] HostName-s01-01 > set cluster configuration unique-ip 1 interface eth1-Mgmt4 ipv4-
addess 172.16.6.186 mask-length 24
1_01:
Adding Alias address 172.16.6.186 of eth1-Mgmt4
1_02:
Adding Alias address 172.16.6.186 of eth1-Mgmt4
2_01:
2_02:
Alias IP was added successfully to Site 1
Alias IP address should be added to the policy rulebase in SmartDashBoard
[Global] HostName-s01-01 >
```

Example 2 - Deleting a UIPS

```
[Expert@HostName-s01-01:0]# gclish
[Global] HostName-s01-01 > delete cluster configuration unique-ip site-id 1 interface eth1-Mgmt4
1_01:
Deleting Alias IP 172.16.6.186 of eth1-Mgmt4
1_02:
Deleting Alias IP 172.16.6.186 of eth1-Mgmt4
2_01:
2_02:
Alias IP of Site 1 was deleted successfully
Alias IP address should be removed from the policy rulebase in SmartDashBoard
[Global] HostName-s01-01 >
```

Managing Orchestrator Ports

You can see the information about Orchestrator Ports and change their settings.

Managing Orchestrator Ports in Gaia Portal

Starting in R82, Gaia Portal shows a dedicated page:

In the **Orchestrator Management** section, click the **Ports** page.

Explanation

The top toolbar shows these items (in the "Table" view):

Icon	Name	Description
	Table	Shows the ports in a table (this is the default view). This table shows: ■ Port Status ■ Physical Port ID ■ Port Type ■ Interface Name in Gaia OS ■ Security Groups, to which this port is assigned ■ Transceiver State ■ MTU ■ QSFP Mode ■ Auto-Negotiation State ■ RX Throughput (frames/sec) ■ TX Throughput (frames/sec) You can right-click a port and click the applicable option: ■ **Edit Port** ■ **Blink LED** ■ **Diagnostics**

Icon	Name	Description
	Map	Shows the ports in a visual map. This map shows a visual representation of the front panel for each Orchestrator on this Site. Different icons on the ports represent different states. The legend for each icon appears in the top right corner. If you left-click a port, then the bottom part of the page shows the port details. You can right-click a port and click the applicable option: ■ **Edit Port** ■ **Blink LED** ■ **Diagnostics**
	Edit	Opens an port configuration window for the selected port. In this window, you can configure these port settings: ■ Change the administrative state of this port on the required Sites ■ Enable or disable the auto-negiotation in this port on the required Sites ■ Configure the MTU ■ Select the port speed (QSFP Mode) ■ Select the port type (Management, Internal Site Sync, External Site Sync, Uplink, Downlink)
	Blink LED	Forces the LED to blink in the selected port. This helps you find this port on the front panel.
	Diagnostics	Runs a short diagnostics on the port.
		Shows the number of ports in the administratively down state.
		Shows the number of ports in the "down" state.
		Shows the number of ports in the "up" state.

Managing Orchestrator Ports in Gaia Clish

Use these commands in Gaia Clish:

- *"add maestro" on page 999*
- *"set maestro" on page 1027*
- *"delete maestro" on page 1012*
- `set interface <Name>`

Monitoring Orchestrator Ports in Gaia Clish

Use these commands in Gaia Clish:

- *"orch_stat" on page 1017*
- *"show maestro" on page 1034*
- `show interface <Name>`
- `show interfaces`

Monitoring Orchestrator Ports in the Expert mode

Use these commands the Expert mode:

- *"orch_stat" on page 1017*
- *"cplink" on page 1003*

System Monitoring in Maestro

This section describes features to monitor your Maestro environment.

For Maestro Orchestrator, see *"SNMP for Maestro Orchestrators" on page 644*.

For Security Groups, see *"Working with SNMP" on page 643*.

SNMP for Maestro Orchestrators

You can use SNMP to monitor different aspects of the Maestro Orchestrator:

- Software versions
- Key performance indicators

Notes:

- Hardware monitoring with SNMP is not supported on Orchestrators..
- For SNMP monitoring of Security Groups, see *"SNMP for Security Groups" on page 647*.
- For SNMP monitoring of Security Group Members, see *"SNMP for Security Group Members" on page 670*.

Prerequisites

Step	Instructions
1	On the Maestro Orchestrator, in Gaia Portal or Gaia gClish: a. Enable the SNMP Agent. b. Configure SNMP settings. **Best Practice** - Use only SNMP v3. See the *R82 Gaia Administration Guide* > Chapter "System Management" > Section "SNMP".

2	Upload these Check Point MIB files from the Security Group to your third-party SNMP monitoring software:
	■ The SNMP MIB file:
	`$CPDIR/lib/snmp/chkpnt.mib`
	■ The SNMP Trap MIB file:
	`$CPDIR/lib/snmp/chkpnt-trap.mib`
	(The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.)

Supported SNMP OIDs for Maestro Orchestrators

Only these OID 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 Maestro Orchestrators

Only these OID 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.

System Optimization in Maestro

This section describes some optimization steps you can take on a Maestro Security Group.

Maestro Auto-Scaling

Introduction to Maestro Auto-Scaling

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 Maestro Orchestrator for each Security Group.

Prerequisites for Maestro Auto-Scaling

- 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 cluster configuration image auto-clone state on
  show cluster configuration 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.
- If the Security Group has internet connectivity, the Scale Unit fetches the license from the User Center. If there is no internet access, you must manually prepare the license by following the instructions in sk180461 before applying the Auto-Scaling feature.

Limitations of Maestro Auto-Scaling

- 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 in Maestro Auto-Scaling

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 of Maestro Auto-Scaling

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
When	**Each Member** 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. **Security Group (Average)** 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.
With	**CPU Utilization (%)** **Throughput (Gbps)** **Packets (p/s)** **Connections** The KPI for the rule.
More than	Configure the threshold between: ■ 1 and 100 for the CPU utilization metric. ■ 1 and 1099511627776 (1TB) for other metrics.
For consecutive period of	Configure the duration between 1 and 86400 seconds (1 day).

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
When	**Security Group (Average)** 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 **less than** the threshold configured in the rule. This means the Security Group can release the current scale unit.
With	**CPU Utilization (%)** **Throughput (Gbps)** **Packets (p/s)** **Connections** The KPI for the rule.
Less than	Configure the threshold between: ■ 1 and 100 for the CPU utilization metric. ■ 1 and 1099511627776 (1TB) for other metrics.
For consecutive period of	Configure the duration between 1 and 86400 seconds (1 day).

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 of Maestro Auto-Scaling 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 of Maestro Auto-Scaling

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
   ```

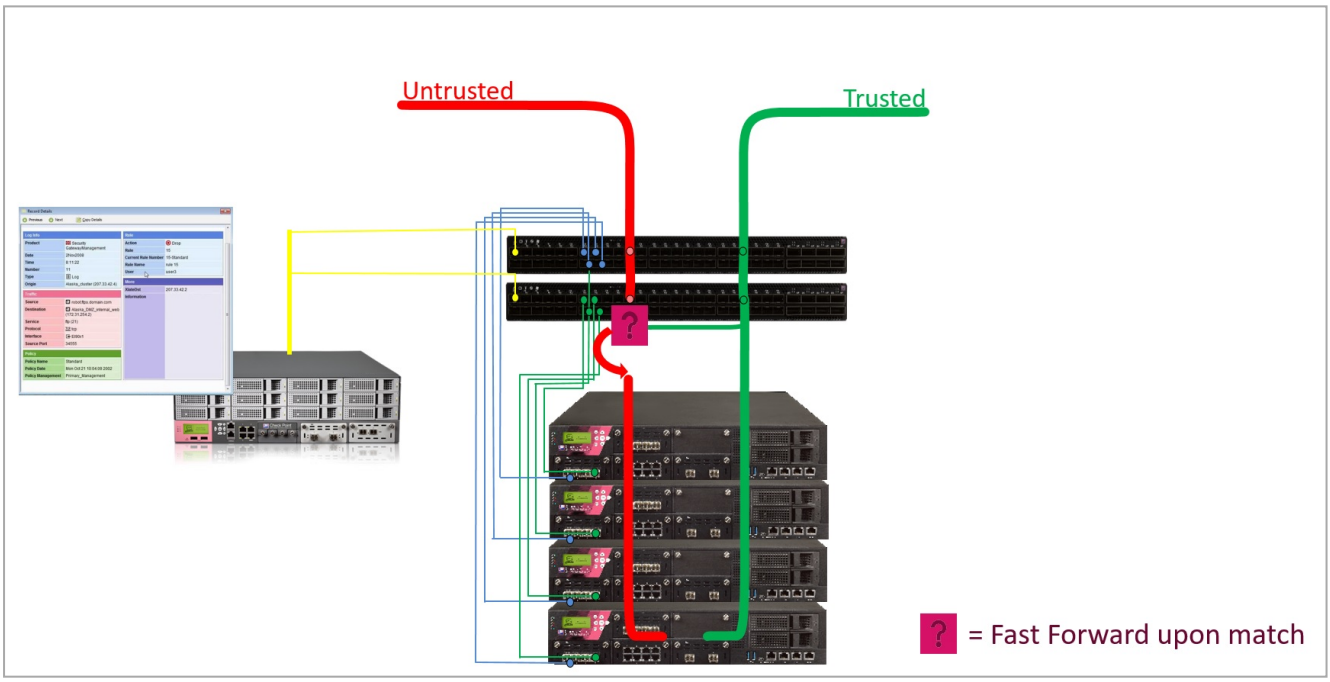
Maestro Fastforward

Introduction to Maestro Fastforward

The Maestro Fastforward feature offloads chosen policy rules for trusted connections to the 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 Maestro Fastforward 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 of Maestro Fastforward" on page 246*.

FAQ for Maestro Fastforward

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 for Maestro Fastforward

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 *"Special Considerations for Maestro Fastforward" on page 243*.
Dual Site	In Dual Site configuration, only "cross-Orchestrator" bond interfaces are allowed **on each site**. Meaning, each bond interface has a subordinate interface on each Orchestrator **on each site**. For more information, see *"Special Considerations for Maestro Fastforward" on page 243*. 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 of Maestro Fastforward

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* (at the top, select the correct version) .

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
Source	■ In the "`Source`" column, you can add one or more objects of these types only: • `Host` • `Network` • `Group` • `Address Range` ■ In the "`Source`" column, you cannot use the object "`Any`". You must add an explicit object. ■ 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). ■ 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.
Destination	■ In the "`Destination`" column, you can add one or more objects of these types only: • `Host` • `Network` • `Group` • `Address Range` ■ In the "`Destination`" column, you cannot use the object "`Any`". You must add an explicit object. ■ 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). ■ 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.

Rule Column	Notes
Services & Applications	■ You can add one or more service objects of type "`TCP`" with these settings: • single port • range of ports • source port ■ You can add one or more service objects of type "`UDP`" with these settings: • single port • range of ports • source port ■ You can add one or more service objects of type "`Other Service`" with an IP-based Protocol.

Notes for rules with the action "Drop"

Note - Orchestrator drops the traffic at an early stage, at the hardware level.

Rule Column	Notes
Source	■ In the "`Source`" column, you can add one or more objects of these types only: • `Host` • `Network` • `Group` • `Address Range` ■ In the "`Source`" column, it is supported to use the object "`Any`". It is not necessary to add an explicit object. ■ 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.

Rule Column	Notes
Destination	■ In the "`Destination`" column, you can add one or more objects of these types only: • `Host` • `Network` • `Group` • `Address Range` ■ In the "`Destination`" column, it is supported to use the object "`Any`". It is not necessary to add an explicit object. ■ 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.
Services & Applications	■ You can add one or more service objects of type "`TCP`" with these settings: • single port • range of ports • source port ■ You can add one or more service objects of type "`UDP`" with these settings: • single port • range of ports • source port ■ You can add one or more service objects of type "`Other Service`" with an IP-based Protocol.

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 of Maestro Fastforward" on page 250*.

   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 Maestro Fastforward

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@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  |
+------------+--------------------+-------------+----------+---------------------------------
-------------------------------------+
```

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`".

Maestro Fastforward Considerations for Administrators

Operation	Regular Flow	Additional Flow
Policy Installation	The Management Server transfers the policy to the Security Group.	The Management Server translates into stateless ACLs the rules that contain the configured prefix in their **Name** column. The Security Group transfers these ACLs to all Orchestrators. If there are no changes in the policy, the Security Group skips this step.
Modifying topology (physical interfaces / routes / bond interfaces)	The administrator adds, modifies, or removes an interface or a route. ■ In Gateway mode, the administrator makes these changes in Gaia gClish / of the Security Group. ■ In VSX mode, the administrator makes these changes in Gaia Portal SmartConsole (except for bond interfaces). When done: ■ In Gateway mode, you must fetch the interface topology and install the policy. ■ In VSX mode, you must install the policy. This makes sure that enforcement is aware of the modifications (Firewall topology, Anti-Spoofing, and more).	During each policy installation, the Security Group transfers the networking topology to all Orchestrators (interfaces, neighbors, static routes). If there are no changes in the topology, the Security Group skips this step.

Routing Mechanism in Maestro Fastforward

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 in Maestro Fastforward

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 Maestro Fastforward" on page 236*):

```
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 for Maestro Fastforward

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:

In a Maestro deployment with multiple Orchestrators, Fastforward requires that all interfaces configured on the Security Group are connected at the active site. This ensures consistent topology visibility across all Orchestrators.

If any interface configured on the Security Group loses connectivity—even one that does not handle important traffic—Fastforward will be disabled, and traffic will be forwarded through the Security Group instead of being accelerated by the Orchestrators.

If a bond interface fails on only one Orchestrator, it creates a topology inconsistency that affects traffic acceleration. In such a case, the Orchestrators on the affected site will enter internal bypass mode.

- Internal Bypass Mode Behavior: In this mode, all traffic is forwarded to the Security Group, bypassing Fastforward acceleration, until topology consistency is restored.
- Restoring Normal Operation: When all interfaces regain connectivity, the Orchestrators exit internal bypass mode and resume their previous state (active/inactive).

Example:

Consider a deployment with two Orchestrators and three bond interfaces:

- Bond1 (External Traffic)
- Bond2 (Critical Internal Traffic)
- Bond3 (Non-Critical Internal Traffic)

Each bond has a total of four subordinate interfaces, split between the two Orchestrators.

If a subordinate interface from Bond3 (which does not handle critical traffic) fails on one Orchestrator:

- Bond2 still has full connectivity
- Bond1 still has full connectivity
- Bond3 is partially disconnected

Since Bond3 does not handle critical traffic, Fastforward should continue functioning.

Because the topology is inconsistent, the Orchestrators enter internal bypass mode, forcing all traffic—including Bond2's critical traffic—through the Security Group. Fastforward is disabled even though the critical traffic paths remain intact.

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 withe lowest ID with the link in the "up" state.

Known Limitations of Maestro Fastforward

General

ID	Description
PMTR-110663	Before you can enable the Fastforward feature, you must make sure that for each configured static route, the Security Group Members learned the MAC Address of the nexthop device and can reach the nexthop device's IP address.
PMTR-76262	Fragments are forwarded to the Security Gateway for rules that contain a service.
PMTR-76274	Complex connections (FTP, SIP, and more) do not open data connections dynamically. In general, there are two options for complex connections: ■ Use the special service for the control connection (examples: FTP port 21, VoIP SIP 5060), and the Security Gateway automatically opens the date connections. ■ Manually allow the control connection (examples: FTP port 21, VoIP SIP 5060) and manually allow the data connection range (example: a UDP port range).

PMTR-108476	**Orchestrator MHO-175 supports a maximum of 10,000 ACL rules.**
	If the Access Control policy was translated into more ACL rules, the Maestro Fastforward feature may stop working during policy installation from the Management Server.
	
	Short-term workaround on the Orchestrator:
	1. Check the current number of ACL rules with this command in the Expert mode:
	`tor_util fastforward show status all all`
	2. Stop the Maestro Fastforward feature with this command in Gaia Clish:
	`set maestro fastforward state off`
	3. Start the Maestro Fastforward feature with this command in Gaia Clish:
	`set maestro fastforward state on`
	
	Long-term workaround on the Management Server:
	Reconfigure the Access Control policy to contain fewer specific rules (for example, for specific Hosts) and to contain more generic rules (for example, for Networks).

ID	Description
-	You must **not** 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 of Maestro Fastforward

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 of Maestro Fastforward" on page 246*.

   - 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 **not** edit this file
Configuration	`/etc/mlx_conf.json`	Fastforward policy information	You must **not** 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 a Dedicated Logging Port in Maestro

The logging mechanism on each Security Group Member in Security Groups forwards the logs directly to a dedicated Log Server over the Maestro Orchestrator's management port assigned to this Security Group.

However, the 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 Maestro Orchestrator's management ports:

1. Assign a dedicated 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
Maestro Orchestrator)[Security Group]
```

```
[Management Server](some interface) <===> (interface 1) [Log Server]
(interface 2) <===> (management port 2 on Maestro Orchestrator)
[Security Group]
```

Procedure:

Step	Instructions
1	Install a dedicated Log Server: a. Install a dedicated Log Server with two physical interfaces. See the applicable *Installation and Upgrade Guide* > Chapter *Installing a Dedicated Log Server or SmartEvent Server.* b. Connect one physical interface on the dedicated Log Server to the Management Server. c. Connect another physical interface on the dedicated Log Server directly to an available management port on the Maestro Orchestrator. **Important** - Do **not** use the same port on the Maestro Orchestrator, which connects to the Management Server. d. In SmartConsole, create the required object that represents the dedicated Log Server. See the applicable *Installation and Upgrade Guide* > Chapter *Installing a Dedicated Log Server or SmartEvent Server.*
2	On the Maestro Orchestrator, assign the dedicated port of type `management` to a Security Group and apply the changes.

Step	Instructions

3	In the Gaia OS of the Security Group, configure in Gaia gClish the dedicated management port.
	Syntax:
	`[Expert@SG-s01-01:0]# gclish`
	`[Global] SG-s01-01> set interface ethX-MgmtY ipv4-address <IPv4 Address> mask-length <Mask Length>`
	Example:
	`[Global] SG-s01-01 > set interface eth1-Mgmt2 ipv4-address 2.2.2.10 mask-length 24`
	Note - You must assign an IPv4 address from the same subnet as assigned to the dedicated interface on the Log Server, which connects to the Maestro Orchestrator.

4	In SmartConsole, configure the Security Group object to send its logs to the dedicated Log Server. See the applicable *Logging and Monitoring Administration Guide* > Chapter *Getting Started* > Section *Deploying Logging Section* - Subsection *Configuring the Security Gateways for Logging*.

Note - The SMO makes sure that return traffic from the Log Server reaches the correct Security Group Member in the Security Group.

Configuring Security Group High Availability in Maestro

Note - Do **not** confuse this section with *"Configuring Weights for Security Group Members in Maestro" on page 174* 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 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:

```
(Unit Weight) x (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 cluster configuration high-availability factors`" command to configure a hardware component's weight.

Syntax in Gaia gClish of the Security Group

```
set cluster configuration high-availability factors member
<Security Group Factor>
```

```
set cluster configuration high-availability factor {other <Other
Port Factor> | standard <Standard Port Factor> | mgmt <Management
Port Factor> | bond <Bond Port Factor>}
```

For more information, see:

- *"show cluster configuration high-availability" on page 960*
- *"set cluster configuration high-availability" on page 925*

Parameters

Parameter	Description
<Security Group 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] SG-s01-01 > set cluster configuration high-availability factors sgm 100
[Global] SG-s01-01 > set cluster configuration high-availability factors port other 70
[Global] SG-s01-01 > set cluster configuration high-availability factors port standard 50
```

Setting the Quality Grade Differential

Description

Use the "`set cluster configuration high-availability failover`" command in Gaia gClish to configure the minimum quality grade differential that causes a failover.

Syntax in Gaia gClish of the Security Group

```
set cluster configuration high-availability failover <Trigger>
```

Parameters

Parameter	Description
<Trigger>	Minimum difference in the Security Group quality grade to trigger a failover. Valid values: 1 - 1000.

Configuring Identity Based Access Control and Threat Prevention in Maestro

For design guidelines, see sk175587.

Configuring Link State Propagation (LSP) on a Maestro Orchestrator

Introduction to LSP

Example traffic flow from a Client to a Server through a Maestro Security Group:

(Client) > (Switch) > (Port 4 on Orchestrator) > (Security Group) > (Port 6 on Orchestrator) > (Switch) > (Server)

- If Port 4 on the Orchestrator goes down, traffic outage occurs.
- If Port 6 on the Orchestrator goes down, traffic outage occurs.

With the Link State Propagation (LSP) feature you can configure these two required ports on the Orchestrator (Port 4 and Port 6) as one LSP Group.

If one of the ports in the LSP Group goes down, then all other ports in the LSP Group go down. As a result, the surrounding switches will not forward traffic for these ports. This eliminates or limits the traffic outage.

Configuration

You configure the LSP Groups in Gaia Clish on the Orchestrator.

Notes:

- You must configure the LSP settings manually on each Orchestrator on each Maestro Site.
- The log file is: `/var/log/lsp_cli.log`

Syntax to add a new LSP Group

```
add maestro lsp
      group <1-1024> [<Port Number 1>,<Port Number 2>,<...>,<Port Number N>]
```

Syntax to configure an existing LSP Group

```
set maestro lsp
      apply
      group <1-1024> ports <Port Number 1>,<Port Number 2>,<...>,<Port Number N>
      revert
      state {on | off}
```

Syntax to show LSP configuration

```
show maestro lsp
      configuration {all | group <1-1024>}
      history <1-1000>
      status
```

Syntax to delete an existing LSP Group or ports from an LSP Group

```
delete maestro lsp
      group <1-1024> [port <Port Number 1>,<Port Number
2>,<...>,<Port Number N>]
```

Parameters

Parameter	Description
`apply`	Applies the changes in the LSP configuration.
`group <1-1024>`	Specifies the ID of the LSP Group. **Important** - The "`set maestro lsp group`" command overwrites the LSP Group if such LSP Group ID already exists.
`ports <Port>,<Port>,...`	Specifies the IDs of the Orchestrator Ports. Press the TAB key to see the available port numbers. To add multiple ports, separate them with commas (`,`) without spaces.
`revert`	Reverts the changes in the LSP configuration that were not applied yet.
`state {on | off}`	Enables (`on`) and disables (`off`) the LSP configuration.
`configuration {all | group <1-1024>}`	Shows the LSP configuration for all LSP Groups or only for the specified LSP Group. The output shows the applied configuration and the changes that were not applied yet.

Parameter	Description
`history <1-1000>`	Show the specified number of the recent LSP events from this log file: `/var/log/lsp_history.log` The output table shows these columns: ■ **Time**: When the event happened. ■ **Port**: The port on which the event has been received. ■ **Event**: The event that occurred. ■ **Group**: The affected LSP group. ■ **Group Status**: The reflection of the event on the LSP group state.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>LSP events:
<table>
<tr><th>Event</th><th>Meaning</th></tr>
<tr><td><code>Down</code></td><td>The port state changed from "up" to "down".</td></tr>
<tr><td><code>admin-down</code></td><td>The port state changed from "up" to "administratively down".
The LSP mechanism forces this state to manage the LSP Groups.</td></tr>
<tr><td><code>recovered down->up</code></td><td>The port state changed from "down" to "up".</td></tr>
<tr><td><code>moved to admin-down, preparing for group recovery</code></td><td>The port state changed from "up" to "administratively down" to prepare the LSP Group for recovery.</td></tr>
<tr><td><code>moved to admin-up</code></td><td>The port state changed from "administratively down" to "administratively up" after preparing the LSP Group for recovery.</td></tr>
<tr><td><code>has recovered after <<i>Time in Seconds</i>></code></td><td>The port state changed (recovered) from "down" to "up" after the specified number of seconds.</td></tr>
<tr><td><code>found down in initializing</code></td><td>While loading the LSP configuration, detected a port in the state "down".</td></tr>
<tr><td><code>admin-down in initializing</code></td><td>While loading the LSP configuration, detected a port in the state "down" and changed its stae from "down" to "administratively down".</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Event</th><th>Meaning</th></tr>
<tr><td><code>Configuration change event received</code></td><td>LSP configuration changed for this specific LSP Group.</td></tr>
<tr><td><code>Resetting ports monitoring</code></td><td>While loading the LSP configuration, started to reassessthe port states (not per port event).</td></tr>
</table>
</td></tr>
<tr><td><code>status</code></td><td>Shows:
The status of the LSP daemon.
If there are configuration changes that were not applied yet.</td></tr>
</table>

Workflow

1. Connect to the command line on **each** Orchestrator.
2. Log in.
3. If your default shell is the Expert mode, then go to Gaia Clish:

   ```
   clish
   ```

4. Create the required LSP Group with the required ports:

   ```
   add maestro lsp group <1-1024> ports <Port Number 1>,<Port Number 2>,...,<Port Number N>
   ```

5. Apply the LSP configuration changes:

   ```
   set maestro lsp apply
   ```

6. Enable LSP:

   ```
   set maestro lsp state on
   ```

7. Examine the LSP configuration:

   ```
   show maestro lsp configuration {all | group <1-1024>}
   ```

Troubleshooting in Maestro

This section provides troubleshooting commands for Maestro.

Note - Maestro Orchestrators do not support the Hardware Diagnostic tool that you run from the Gaia OS Boot Menu (Known Limitation MBS-17809).

Installing the Gaia Operating System on a Maestro Orchestrator

To perform a clean installation of the Gaia Operating System on a Maestro Orchestrator, you can:

- Restore your 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 Maestro Orchestrator to the last Gaia that was installed using the Clean Install method.

Step	Instructions
1	Connect to the Maestro Orchestrator using the serial console.
2	Log in to the Gaia Clish.
3	Restart the Maestro Orchestrator. Run: `reboot`

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:
	`Loading the system`
	`Press any key to see the boot menu [Booting in 5 seconds]`

5	In the menu, select **Reset to factory defaults** and press Enter.
6	Type **yes** and press Enter.
7	Wait for the Maestro Orchestrator to boot.
8	With a web browser, connect to the Gaia Portal on the Maestro Orchestrator: `https://<IP Address of MGMT Port>`
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 *Check Point Support* to configure the Maestro Orchestrator to boot from the USB device by default.
2	Download the required Clean Install package (ISO) for Maestro Orchestrators from sk181127.
3	Follow sk65205 to create a bootable USB device. **Important:** ▪ Always use the latest available build of the ISOmorphic Tool. If you use an outdated build, the installation can fail. ▪ Select the option **Open Server with console**.
4	Insert the bootable USB device into the Maestro Orchestrator.
5	Connect to the Maestro Orchestrator through the console port.
6	Restart the Maestro Orchestrator. Run: `reboot`
7	Wait for the Maestro Orchestrator to boot from the USB device.
8	Select the boot option **Open Server with console**.
9	Install the Gaia Operating System.
10	**Before the reboot, remove the USB device.**
11	Confirm the reboot.
12	With a web browser, connect to the Gaia Portal on the Maestro Orchestrator: `https://<IP Address of MGMT Port>`
13	Run the Gaia First Time Configuration Wizard.

Log and Configuration Files in Maestro

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.*` (in the context of each Virtual System)
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/smartd.log.dbg` Also, run the `lldpneighbors` command
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 Maestro Orchestrators

Feature	File
All logs that do not have a dedicated log file	`/var/log/junk.log.dbg`
Applying Security Group configuration	`/var/log/ssm_sg.log.dbg`
Configuring the SDK	`/var/log/messages`
Information about Security Groups	`/etc/sgdb.json`
Information about detected Security Group Members	`/etc/rsrcdb.json`
LLDP updates	`/var/log/smartd.log.dbg` Also, run the `lldpctl` command
Starting of the SDK	`/var/log/start_tor_ssm.log.dbg`

Replacing a Maestro Orchestrator

Follow the steps in sk174202.

Working with Quantum Scalable Chassis

Note - This chapter describes the unique procedures that apply only to Scalable Chassis 44000 / 64000.
For additional procedures that apply to all Scalable Platforms, see the chapter *"Common Procedures for Scalable Platforms" on page 504*.

Scalable Chassis Overview

Scalable Chassis are built for demanding environments and are based on proven technologies used by Fortune 100 companies and telecommunication vendors all over the world.

The ATCA-compliant, carrier-grade design offers scalability, availability, and serviceability with high performance and high port density.

Redundant Security Switch Modules (SSMs) provide switching fabric, physical interface, and routing functions.

Redundant Chassis Management Modules (CMMs) continuously check and monitor the health of the chassis including fans, power supplies, and Security Gateway Modules (SGMs).

For optimal reliability:

- Check Point ClusterXL Load Sharing distributes the load between Security Gateway Modules in one chassis.
- Check Point ClusterXL High Availability operates between chassis on the same or different sites (a Dual Chassis configuration eliminates down-time).

The Check Point SyncXL technology provides highly efficient synchronization of system and security information between components to ensure high system performance.

Action Plan:

1. Connect Scalable Chassis on your network.
2. On **one** of the Scalable Chassis, configure the applicable Security Group.
3. In SmartConsole:
   a. Configure a single Security Gateway object (the Single Management Object, SMO) that represent this Security Group.
   b. Configure and install the applicable Security Policies on this Security Gateway object.
4. On the Security Group, configure other applicable settings (for example, routing).
5. Add other Security Gateway Modules to the chassis, as needed.

   The Security Gateway Modules automatically clone all software packages, settings, and security policies from the SMO Security Group Member.

For the initial installation and configuration, see the *Scalable Chassis Getting Started Guide*.

Introduction to Scalable Chassis

Introducing the Check Point Scalable Chassis, the world's fastest Threat Prevention platforms.

The carrier-class next generation Threat Prevention and Firewall solutions, provide the security you need today and into the future.

Already supporting fast networking connectivity such as 40 GbE and 100 GbE, the 64000 and 44000 can be integrated with new and advanced solutions, both on premises or in the cloud.

These Chassis let you continue to grow your business, so when traffic volume or security requirements increase, you can easily scale up the system capacity.

Welcome to the future of Cyber Security!

Licensing

For information on how to manage licenses, see:

- *"Step 5: Licensing and Registration on Scalable Chassis" on page 315*.
- The *R82 Gaia Administration Guide* > Chapter "**Maintenance**" > Section "**License Status**".

Run all licensing commands in Gaia gClish of the applicable Security Group.

Upgrading Scalable Chassis to R82 - Zero Downtime (MVC)

This section describes the steps for upgrading a Scalable Chassis environment with Zero Downtime - as a Multi-Version Cluster (MVC).

This procedure supports only these upgrade paths for Security Groups:

- from R81.20 to R82
- from R81.10 to R82

Important - See this rollback procedure - *"Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC)" on page 505*.

Important Notes for Security Groups:

- Before you upgrade the Security Groups, you must upgrade the Management Server that manages the Security Groups.
  See the *R82 Installation and Upgrade Guide*.
- This procedure applies to Security Groups in the Gateway mode and the Traditional VSX mode.
  In Traditional VSX mode, you must run all the commands in the context of VS0:
  - To change the context in Gaia gClish, run: `set virtual-system 0`
  - To change the context in the Expert mode, run: `vsenv 0`
- **During the upgrade process, it is:**
  - **Forbidden to change the configuration of the Security Group and its Security Group Members.**
- 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	• 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.
Single Site	• 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 from 1_4 to 1_5.

Environment	Description
Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.

- 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 the Security Group.
    2. If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish:
       ```
       gclish
       ```
    3. Get the current Active/Standby mode and write it down (you need it at the end of the procedure):
       ```
       show chassis high-availability mode
       ```
       Available Modes:

Mode ID	Mode Title	Mode Description
0	**Active/Standby - Active Up**	No primary Site. The currently Active Site stays Active until one of these changes: ◦ The currently Active Site changes its state to "DOWN". If the formerly Active Site changes its state to "UP" again, it becomes the Standby Site. ◦ The quality grade of the currently Standby Site becomes greater than the quality grade of the currently Active Site.
1	**Active/Standby - Primary Up**	The Active Site always stays Active until one of these changes: ◦ The currently Active Site changes its state to "DOWN". If the formerly Active Site changes its state to "UP" again, it becomes the Active Site again. ◦ The quality grade of the currently Standby Site becomes greater than the quality grade of the currently Active Site.
2	Not available	Not supported. This mode is reserved.
3	**Standby Chassis VSLS Mode**	In the Traditional VSX mode, provides Virtual System Load Sharing.

4. Decide which of the Site should be Active for this procedure.
5. Change the Active/Standby mode to "**Active/Standby - Primary Up**" (value "1"):

```
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 Standby Site, change the Active/Standby mode to "**Active/Standby - Primary Up**" (value "1"):

```
set cluster configuration high-availability
mode 1
```

9. On the upgraded Site change the Site Priority - enter the number of the currently Active Site:

```
set cluster configuration high-availability
vs site_priority {1 | 2}
```

10. Upgrade all Security Group Members on the new Standby Site (former Active Site).
11. Change the Active/Standby mode to the previous mode:

```
set cluster configuration high-availability
mode <Mode ID>
```

Required software packages:

Download the required software packages from sk181127:

1. The required CPUSE Deployment Agent.
2. The required Take of the Jumbo Hotfix Accumulator for the current version.
3. The R82 Upgrade Package for Scalable Platforms.

Workflow:

1. On the Management Server - Upgrade to the required version that can manage an R82 Security Group (see sk113113).
2. On the Security Group - Run the Pre-Upgrade Verifier to make sure it is possible to upgrade the Security Group.
3. On the Security Group - Install the required Jumbo Hotfix Accumulator (using two logical groups of Security Group Members).
4. On the Security Group - Install the required CPUSE Deployment Agent package.
5. On the Security Group - Upgrade to R82 (using two logical groups of Security Group Members).
6. In SmartConsole, install the policy.

Procedure:

Step 1 - Upgrade the Management Server

Upgrade the Security Management Server / Multi-Domain Security Management Server to the required version that can manage an R82 Security Group.

See the *R82 Release Notes* or sk113113.

Step 2 - On the Management Server, change the version of the Legacy VSX Gateway object

Important - This step applies **only** when the Security Group works in the Traditional 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: `mdsenv <IP Address or Name of Domain Management Server>`
D	Upgrade the version of a VSX Gateway object in the management database: **Warning** - Make sure to close all SmartConsole clients connected to this Management Server. `vsx_util upgrade [-s <Mgmt Server>] [-u <UserName>]` For more information, see the *R82 VSX Administration Guide* > Chapter "Command Line Reference" > Section "vsx_util".
E	Log in with the Management Server administrator credentials.
F	Select the Traditional VSX Gateway object for this Security Group.
G	Change the version to **R82**. Follow the instructions on the screen.

Step 3 - 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set smo image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show smo image auto-clone state`

Step 4 - 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 sk181127:

- On a Maestro Security Group:

  "Installing a Hotfix Package on Security Group Members" on page 519

- On a Scalable Chassis:

  "Installing and Uninstalling a Hotfix on SGMs on Scalable Chassis" on page 317

Step 5 - 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 required CPUSE Deployment Agent package (from sk92449) 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 Gaia gClish (`/etc/gcli.sh`), then go to the Expert mode: `expert`
D	Make sure the CPUSE Deployment Agent package exists: `ls -l /<Full Path>/<Name of CPUSE Deployment Agent Package>`

E	Upgrade the CPUSE Deployment Agent:
	`update_sp_da /<Full Path>/<Name of CPUSE Deployment Agent Package>`
	Example:
	`update_sp_da /var/log/DeploymentAgent_XXXXXXXXX.tgz`

F	Make sure all Security Group Members have the same build of the CPUSE Deployment Agent: `gclish -c "show installer status build"`

Step 6 - On the Security Group, import the R82 upgrade package

Step	Instructions
A	Make sure you have the applicable CPUSE Offline package: *R82 Upgrade Package for Scalable Platforms*
B	Transfer the CPUSE Offline package to the Security Group (into some directory, for example `/var/log/`).
C	Connect to the command line on the Security Group.
D	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`
E	If you enabled MDPS (sk138672) on the Security Group, then go to the Management Plane: `set mdps environment mplane`

F	Import the CPUSE Offline package from the hard disk:
	`installer import local /<Full Path>/<Name of the CPUSE Offline Package>`
	Example:
	`[Global] HostName-s01-01 > installer import local /var/log/Check_Point_R82_Gaia_Install_and_Upgrade.tar`

G	Show the imported CPUSE packages: `show installer packages imported`

Step	Instructions

H	Make sure the imported CPUSE package can be installed on this Security Group:
	`installer verify [Press Tab]`
	`installer verify <Number of CPUSE Package> member_ids all`
	Example:
	`[Global] HostName-s01-01 > 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-s01-01 >`

Step 7 - On the Security Group, upgrade the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**A**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**B**" **over SSH**.

B	Go to the context of one of the Security Group Members in the Logical Group "A":
	`member <Member ID>`
	Example:
	`member 1_1`

C	If your default shell is Gaia gClish (`/etc/gcli.sh`), then go to the Expert mode: `expert`

D	Set the Security Group Members in the Logical Group "A" to the state "`DOWN`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "`g_clusterXL_admin`" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "A"> down`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "A"> down`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_1 down`
	`g_clusterXL_admin -b 1_2 down`
	`g_clusterXL_admin -b 1_3 down`
	`g_clusterXL_admin -b 1_4 down`

Step	Instructions
E	Examine the state of the Security Group Members: `asg monitor` The state of the Security Group Members must be: ■ In the Logical Group "**A**" - "**DOWN**". ■ In the Logical Group "**B**" - "**ACTIVE**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

F	Go from the Expert mode to Gaia gClish:
	■ If your default shell is the Expert mode (`/bin/bash`), then run:
	`gclish`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`), then run:
	`exit`

G	Upgrade the Security Group Members in the Logical Group "A":
	`installer upgrade [Press the Tab key]`
	`installer upgrade <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] HostName-s01-01 > 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) y`
	`[Global] HostName-s01-01 >`

Step	Instructions

H	Go from Gaia gClish to the Expert mode:
	■ If your default shell is the Expert mode (`/bin/bash`), then run:
	`exit`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`), then run:
	`expert`

I	Monitor the Security Group Members in the Logical Group "A" until they boot: `asg monitor` **Important:** ■ By design, the upgraded Security Group Members boot into the state "**DOWN(Policy)(R82)**" because the Critical Device "**Policy**" reports its state as "`problem`" (you can run the "`cluster-cli show info pnotes`" command). ■ In the Traditional VSX mode, the Security Group Members are pulling the policy automatically from Management Server during their boot. **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

Step 8 - 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 Traditional 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 **Gateways & Servers**.
C	Double-click the Security Gateway object for this Security Group.
D	In the left tree, click **General**.
E	In the **Version** field, select **R82**.
F	Click **OK**.
G	Publish the session.
H	Install the Access Control policy on this Security Gateway object. **Important** - You must **disable** the Accelerated Policy Installation as described in sk168055: i. Click **Install Policy**. ii. In the **Install Policy** window, right-click on the Security Gateway object. iii. Select **Do not use Install Policy Acceleration for all gateways**. iv. Select the Security Gateway object. v. Click **Install**. **Notes:** ■ Only the upgraded R82 Security Group Members install this policy. The Security Group Members that still run the previous version ignore this policy installation. ■ If the policy installation fails, refer to sk184660.

Step	Instructions
I	On the Security Group (in the Expert mode), examine the state of the Security Group Members: `asg monitor` The state of the Security Group Members must be: ■ In the upgraded Logical Group "**A**" - "**DOWN(READY)(R82)**". ■ In the Logical Group "**B**" - "**ACTIVE(<previous version>)**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

Step 9 - On the Security Group, change the state of Security Group Members in the Logical Group "A" to "Up"

Step	Instructions

A	Set the Security Group Members in the Logical Group "A" to the state "`UP`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "`g_clusterXL_admin`" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "A"> up`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "A"> up`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_1 up`
	`g_clusterXL_admin -b 1_2 up`
	`g_clusterXL_admin -b 1_3 up`
	`g_clusterXL_admin -b 1_4 up`

B	Examine the state of the Security Group Members: `asg monitor` The state of the Security Group Members must be: ■ In the upgraded Logical Group "**A**" - "**ACTIVE(R82)**". ■ In the Logical Group "**B**" - "**ACTIVE(<previous version>)**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

Note - Because of the Multi-Version Cluster (MVC) mechanism design, the upgraded Security Group Members also process the traffic.

Important - If this Security Group works in the Traditional VSX mode, the state of the upgraded Security Group Members may remain "**DOWN**" because the Critical Device "`DSD`" reports its state as "`problem`" (run the "`show cluster info pnotes`" command).
This issue may occur if before the upgrade you configured **static** CoreXL Affinity with the command "`fw ctl affinity -s -d -fwkall <Number of CPUs>`" (to see the current configuration, run the command "`fw ctl affinity -l -x`").
Follow these workaround steps:

1. Connect to the command line on the Security Group.
2. If the default shell is the Expert mode, then go to Gaia gClish:

   ```
   gclish
   ```

3. Disable the CoreXL Dynamic Balancing:

   ```
   set dynamic-balancing state disable
   ```

4. Reboot the upgraded Security Group Members:

   ```
   reboot -b <SGM IDs>
   ```

5. Examine the state of the upgraded Security Group Members:

   ```
   show cluster info pnotes
   ```

   ```
   asg monitor
   ```

Step 10 - On the Security Group, change the state of Security Group Members in the Logical Group "B" to "Down"

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: ■ Connect to one of the Security Group Members in the Logical Group **"B" through the console**. ■ Connect to one of the Security Group Members in the Logical Group **"A" over SSH**.

B	Set the Security Group Members in the Logical Group "B" to the state "DOWN":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "g_clusterXL_admin" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "B"> down`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "B"> down`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_5 down`
	`g_clusterXL_admin -b 1_6 down`
	`g_clusterXL_admin -b 1_7 down`
	`g_clusterXL_admin -b 1_8 down`

Note - At this time, the Security Group runs only with the upgraded Security Group Members.
You can perform the required tests on your network to make sure the new version works as expected.
If there are any issues:

1. Set the Security Group Members in the Logical Group "B" to the state "UP".
2. Set the Security Group Members in the upgraded Logical Group "A" to the state "DOWN".

Step 11 - On the Security Group, upgrade the Security Group Members in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**B**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**A**" **over SSH**.

B	Go to the context of one of the Security Group Members in the Logical Group "B":
	`member <Member ID>`
	Example:
	`member 1_5`

C	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`

D	Upgrade the Security Group Members in the Logical Group "B":
	`installer upgrade [Press the Tab key]`
	`installer upgrade <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] HostName-s01-01 > 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) y`
	`[Global] HostName-s01-01 >`

E	Go from Gaia gClish to the Expert mode:
	■ If your default shell is the Expert mode (`/bin/bash`), then run:
	`exit`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`), then run:
	`expert`

Step	Instructions
F	Monitor the Security Group Members in the Logical Group "B" until they boot: `asg monitor` The state of the Security Group Members must be: ■ In the Logical Group "**A**" - "**ACTIVE(R82)**". ■ In the Logical Group "**B**" - "**DOWN(READY)(R82)**". **Warning** - During this upgrade procedure, do **not** use the "`insights`" command to monitor the state of Security Group Members (Issue ID PMTR-122288).

G	Set the Security Group Members in the Logical Group "B" to the state "`UP`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	Warning - During this upgrade procedure, you **must** use only the "`g_clusterXL_admin`" command in the Expert mode to change the state of Security Group Members.
	Syntax:
	`g_clusterXL_admin -b <ID of first selected SGM in Group "B"> up`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "B"> up`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_5 up`
	`g_clusterXL_admin -b 1_6 up`
	`g_clusterXL_admin -b 1_7 up`
	`g_clusterXL_admin -b 1_8 up`

Step 12 - 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 Gaia gClish (`/etc/gcli.sh`), then go to the Expert mode: `expert`
C	Examine the state of the Security Group Members: `asg monitor` Each Security Group Members must have the state "**ACTIVE**".
D	Run this command (see *"hcp" on page 899*): `hcp -m all -r all`

Initial Software Installation and Configuration on Scalable Chassis

This chapter contains the required steps to install your Scalable Chassis.

Step 1: Installing the SGM Image on Scalable Chassis

Use one of these procedures to install an image on the Security Gateway Modules (SGMs):

- Using an ISO image on a removable media (DVD or USB)
- Using a snapshot import
- Scalable Chassis 44000 support PXE installation on Slot 6 (SGM 2_06 / SGM 1_06) by changing the `kdevice` to `eth3`.

Installing the SGM Image from a Removable Media

You can install an ISO image on the SGMs from a USB stick or DVD.

To copy the ISO image to a removable media:

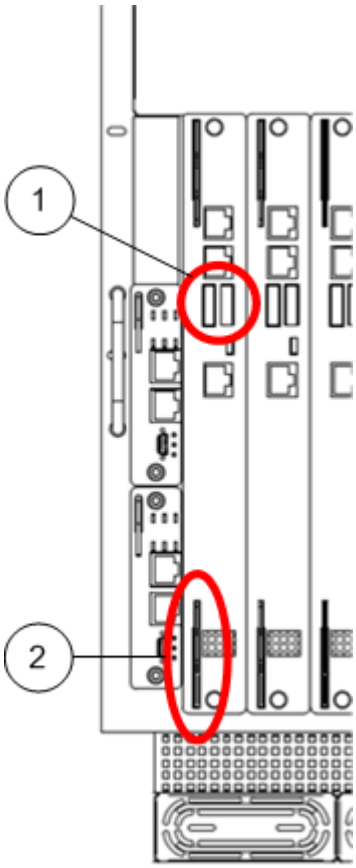
Step	Instructions
1	Download the ISO image file from the R82 Home Page for Chassis: sk181127.
2	Copy the file to a removable media in one of these ways: ■ Burn the ISO file to a DVD. ■ Download the Check Point ISOmorphic tool to create a bootable USB device from the ISO. See sk65205. Make sure that your USB device is compatible with ISOmorphic. See sk92423 for details.
3	You can install many SGMs at one time. Copy the ISO image to many USB sticks or DVDs.

To install an ISO image on the SGMs:

Step	Instructions
1	Connect the removable media to the **left-most** SGM on the Chassis in one of these ways: ■ Connect the USB stick to the USB port. ■ Connect an external DVD drive to the USB port. Put the DVD with the ISO file in the DVD drive.
2	Connect the supplied DB9 serial cable to the console port on the front of the **left-most** SGM on the Chassis.
3	Connect to the left-most SGM using a terminal emulation program.
4	Reboot the SGM by partially sliding it out and immediately pushing it back in place: a. Loosen the thumb screws at the top and bottom of the SGM. b. Open the latches at the top and bottom of the SGM. c. Partially slide out the SGM. d. Push back the SGM. e. Fasten the latches. f. Tighten the thumb screws.
5	When the first screen appears in the terminal emulation program, select **Install Gaia on the system** and press **Enter**. **Important** - If you do not press **Enter** within 60 seconds, SGM starts from the hard drive. The timer countdown stops once you press **Enter**. There is no time limit for the subsequent steps.
6	Press **OK** to continue with the installation. After the installation, the Chassis begins the boot process, and status messages appear in the terminal emulation program.

Step	Instructions
7	Install the SGM image on the other SGMs. To install on one SGM at a time, repeat all the steps for each SGM. To install on many SGMs at the same time: a. Insert all the USB sticks or DVD drives into the USB ports of the other SGMs. b. Follow these steps for one SGM at a time: i. Connect over the console port to the SGM. ii. Reboot the SGM by partially sliding it out and immediately pushing it back in place. iii. Select **Install Gaia on the system** and press **Enter**.

Example:



Item	Description
1	USB port
2	One of two latches for extracting and inserting the SGM

Upgrading the SGM220 BIOS Firmware

To upgrade the BIOS:

Step	Instructions
1	Copy the BIOS file (the file name contains the string "`hpm1bios`").
2	Connect to the SGM over the SSH or console.
3	Go to the directory with the BIOS file.
4	Upgrade the BIOS firmware: `ipmitool hpm upgrade <BIOS Firmware File> [all]` See the example below. **Note** - When the firmware update modifies the device ID, the `ipmitool` must include the "`all`" parameter.
5	Load the default CMOS settings from the new BIOS image uploaded before: `ipmitool raw 0x2e 0x81 0x39 0x28 0x00` See the example below.
6	Reboot the SGM in one of these ways: ▪ Sliding it out and immediately push it back in place ▪ Run this command from the SGM that runs as the SMO: `ccutil restart_sgm sgm_number`
7	Repeat the upgrade process for the backup BIOS firmware.

To see the SGM firmware file, go to this directory:

```
$FWDIR/conf/hw_firmware/SGM220/
```

Example:

```
# ipmitool hpm upgrade 5322H120_cp_a20_hpm1bios.img all

PICMG HPM.1 Upgrade Agent 1.0.2:

Validating firmware image integrity...OK
Performing preparation stage...
Services may be affected during upgrade. Do you wish to continue? y/n y
OK

Performing upgrade stage:

--------------------------------------------------------------------------------
|ID | Name. ....|  Versions..........   |    Upload Progress  | Upload| Image |
|   |           | Active| Backup| File  |0%     50%    100%   | Time  | Size  |
|---|-----------|-------|-------|-------||----+----+----+----||-------|-------|
|*4 |5322 BIOSS |  1.10 |  1.00 |  1.20 ||                   || 12.18 | 20001c|
--------------------------------------------------------------------------------
(*) Component requires Payload Cold Reset

Firmware upgrade procedure successful

# ipmitool raw 0x2e 0x81 0x39 0x28 0x00
 39 28 00
```

Step 2: Connecting Scalable Chassis to the Network

Step	Instructions
1	Connect the serial cable to the applicable CMM console port on the Control Panel.
2	Connect the management ports on the Security Switch Modules to your network.
3	Connect the data ports on the Security Switch Modules to your network.

For more information, see the *Scalable Chassis Getting Started Guide*:

Step 3: Initial Software Configuration on Scalable Chassis

When you install and configure the Chassis, start with the Security Gateway Module (SGM) #1 in the Slot #1 (see the *Scalable Chassis Getting Started Guide* > Chapter *Hardware Components*.).

After you configure the first SGM, it automatically propagates the installation and configuration settings to all other SGMs in the defined *Security Group*.

The Security Group is the group of SGMs that make up the Security Gateway.

Note - In SmartConsole, one Security Gateway (or Legacy VSX Gateway) object represents all the SGMs in the applicable Security Group.

Step 4: Configuration of Scalable Chassis in SmartConsole

A Security Group on Scalable Chassis can work as a Security Gateway, or as a Legacy VSX Gateway.

Note - In SmartConsole, one Security Gateway (or Legacy VSX Gateway) object represents all the SGMs in the applicable Security Group.

Follow one of these procedures:

- *"Configuring a Security Gateway Object for Scalable Chassis in SmartConsole" on page 302*
- *"Configuring a Legacy VSX Gateway Object for Scalable Chassis in SmartConsole" on page 307*

Configuring a Security Gateway Object for Scalable Chassis in SmartConsole

In This Section:

A Security Group on Scalable Chassis can work as a Security Gateway, or as a Legacy VSX Gateway.

This procedure describes the configuration of a Security Gateway in SmartConsole.

Note - There can be some variations in the wizard steps due to release updates. In these cases, follow the instructions on the screen.

Configuring a Security Gateway Object

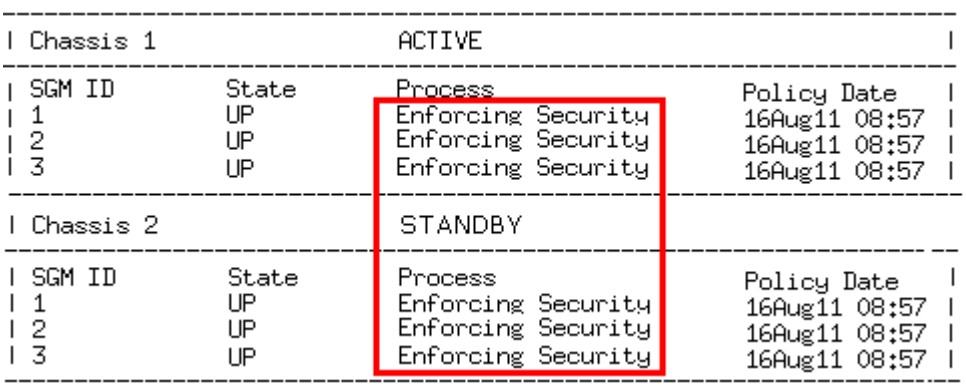
Step	Instructions
1	Connect with SmartConsole to your Management Server.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New (✳) > Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > Gateway**.
4	In the **Check Point Security Gateway Creation** window, select **Wizard Mode** or **Classic Mode**. This procedure describes the **Wizard mode**. If you choose **Classic Mode**, make sure you set all the necessary configuration parameters.

Step	Instructions
5	On the **General Properties** page: a. In the **Gateway name** field, enter the applicable name for this Security Gateway object. b. In the **Gateway platform** field, select the correct chassis. c. In the **Gateway IP address** section, select the applicable option: ■ If you selected **Static IP address**, configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** 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. ■ If this Security Group receives its IP addresses from a DHCP server, click **Cancel**. Create a new Security Gateway object and in the **Check Point Security Gateway Creation** window, select **Classic Mode**. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select the applicable option: ■ If you selected **Initiate trusted communication now**, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. ■ If you selected **Skip and initiate trusted communication later**, make sure to follow Step 7. b. Click **Next**.
7	On the **End** page: 1. Examine the **Configuration Summary**. 2. Select **Edit Gateway properties for further configuration**. 3. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.

Step	Instructions
8	If during the Wizard Mode, you selected **Skip and initiate trusted communication later**: 1. The **Secure Internal Communication** field shows `Uninitialized`. 2. Click **Communication**. 3. In the **Platform** field, select **Open server / Appliance**. 4. Enter the same **Activation Key** you entered during the Security Gateway's First Time Configuration Wizard. 5. Click **Initialize**. Make sure the **Certificate state** field shows `Established`. 6. Click **OK**.
9	On the **General Properties** page: ■ On the **Network Security** tab, enable the applicable Software Blades. ■ On the **Threat Prevention** tab, enable the applicable Software Blades.
10	In the navigation tree, select **Topology**. Configure: ■ Topology of Interfaces as Internal or External. ■ Anti-Spoofing. **Note**- Only data and management interfaces show in the list.
11	Click **OK**
12	Publish the SmartConsole session.
13	Configure the applicable Security Policy for the Security Gateway in SmartConsole: a. From the left navigation panel, click **Security Policies**. b. Create a new policy and configure the applicable layers: i. At the top, click the **+** tab (or press **CTRL T**). ii. On the **Manage Policies** tab, click **Manage policies and layers**. iii. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. iv. Click **Close**. v. On the **Manage Policies** tab, click the new policy you created. c. Create the applicable Access Control rules. d. Install the Access Control Policy on the Security Gateway object. e. Create the applicable Threat Prevention rules. f. Install the Threat Prevention Policy on the Security Gateway object.

Confirming the Policy Installation

To make sure that the policy was installed successfully:

Step	Instructions
1	Connect to one of the SGMs over SSH or a serial console.
2	Run: `asg monitor`
3	Make sure that the SGM status is "**Enforcing Security**" on the ACTIVE and STANDBY Standby Chassis. Example: 
4	Make sure the **Policy Date** matches the date and time the policy was installed.

```
-------------------------------------------------------------------
| Chassis 1                ACTIVE                                 |
-------------------------------------------------------------------
| SGM ID       State       Process                 Policy Date    |
| 1            UP          Enforcing Security      16Aug11 08:57  |
| 2            UP          Enforcing Security      16Aug11 08:57  |
| 3            UP          Enforcing Security      16Aug11 08:57  |
-------------------------------------------------------------------
| Chassis 2                STANDBY                                |
-------------------------------------------------------------------
| SGM ID       State       Process                 Policy Date    |
| 1            UP          Enforcing Security      16Aug11 08:57  |
| 2            UP          Enforcing Security      16Aug11 08:57  |
| 3            UP          Enforcing Security      16Aug11 08:57  |
-------------------------------------------------------------------
```

Confirming the Security Gateway Software Configuration

To make sure the software configuration is correct:

Step	Instructions
1	Connect to one of the SGMs over SSH or a serial console.

2	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Use the command to collect and show diagnostic information about the system.

If there is a problem, fix it before using the system.

Configuring a Legacy VSX Gateway Object for Scalable Chassis in SmartConsole

In This Section:

A Security Group on Scalable Chassis can work as a Security Gateway, or as a Legacy VSX Gateway (Scalable Chassis does not support the VSNext mode).

This procedure describes the configuration of a Legacy VSX Gateway in SmartConsole.

Important - While running Legacy VSX Gateway Wizard, only one SGM (SMO) should be defined in the Security Group.

Before creating the Legacy VSX Gateway

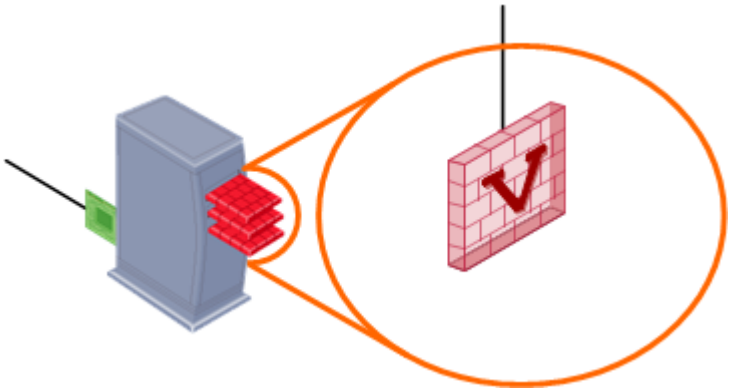
It is important to know how Traditional VSX works, and understand the Traditional VSX architecture and concepts. It is also important to understand how to deploy and configure your security environment using VSX Virtual Devices:

- Virtual System
- Virtual System in Bridge Mode
- Virtual Switch

To learn about how VSX works, architecture, concepts and Virtual Devices, see the *R82 VSX Administration Guide*.

The VSX Gateway Wizard

The VSX Gateway in this example has one Virtual System (VS0) and one dedicated management interface.



After you complete the VSX Gateway Wizard, you can change the VSX Gateway definition from SmartConsole.

For example, you can add Virtual Systems, add or delete interfaces, or configure existing interfaces to support VLANs.

Notes:

1. Do not enable IPv6 before you create and configure a new VSX Gateway. This can cause system instability.
   You must first create the new VSX Gateway object, and then enable and configure IPv6 in Gaia gClish on the Security Group.
2. There can be some variations in the wizard steps due to release updates.
   In these cases, follow the instructions on the screen.

To start the VSX Gateway wizard:

Step	Instructions
1	Connect with SmartConsole to your Management Server.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new VSX Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) **> VSX > Gateway**. ■ In the top left corner, click **Objects** menu **> More object types > Network Object > Gateways and Servers > VSX > New Gateway**. ■ In the top right corner, click **Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Gateway**. The **VSX Gateway Wizard** opens.

Wizard Step 1: Defining VSX Gateway General Properties

On the **VSX Gateway General Properties (Specify the object's basic settings)** page:

1. In the **Enter the VSX Gateway Name** field, enter the applicable name for this VSX Gateway object.
2. In the **Enter the VSX Gateway IPv4** field, enter the same IPv4 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard.
3. In the **Enter the VSX Gateway IPv6** field, enter the same IPv6 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard.
4. In the **Select the VSX Gateway Version** field, select **R82**.
5. Click **Next**.

Wizard Step 2: Selecting Virtual Systems Creation Templates

On the **Virtual Systems Creation Templates (Select the Creation Template most suitable for your VSX deployment)** page:

1. Select the applicable template.
2. Click **Next**.

The **Creation Templates** page determines predefined, default topology, and routing definitions for Virtual Systems.

This makes sure that Virtual Systems are consistent and makes the definition process faster.

You always have the option to override the default creation template when you create or change a Virtual System.

The creation templates are:

- **Shared Interface**- Not supported for the Chassis.
- **Separate Interfaces** - Virtual Systems use their own separate internal and external interfaces. This template creates a **Dedicated Management Interface** (DMI) by default.
- **Custom Configuration** - Defines Virtual System, Virtual Switch, and Interface configurations.

This procedure describes the **Custom Configuration** template.

Wizard Step 3: Establishing SIC Trust

On the **VSX Gateway General Properties (Secure Internal Communication)** page:

1. In the **Activation Key** field, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard.
2. In the **Confirm Activation Key** field, enter the same Activation Key again.
3. Click **Initialize**.
4. Click **Next**.

If you entered the correct activation key, the **Trust State** changes to "`Trust established`".

Wizard Step 4: Defining Physical Interfaces

On the **VSX Gateway Interfaces (Physical Interfaces Usage)** page:

1. Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway.
2. If you plan to connect more than one Virtual System directly to the same physical interface, you must select **VLAN Trunk** for that physical interface.
3. Click **Next**.

Virtual Network Device Configuration

Notes:

- If earlier you selected the **Separate Interfaces** template, proceed to *"Wizard Step 5: VSX Gateway Management" on the next page*.
- If earlier you selected the **Custom Configuration** template, the **Virtual Network Device Configuration** window opens.
  In this window, define a Virtual Device with an interface shared with the VSX Gateway.
  If you do not want to define a Virtual Device at this time, click **Next** to continue.

To define a Virtual Device with a shared interface:

Step	Instructions
1	Select **Create a Virtual Device**.
2	Select the **Virtual Network Device type** > **Virtual Switch**.
3	Select the **shared physical interface** to define a non-DMI gateway. Do **not** select the management interface, if it is necessary to define a **Dedicated Management Interface (DMI)** gateway. If you do not define a shared Virtual Device, a DMI gateway is created by default. **Important** - It is not possible to change this setting after you complete the VSX Gateway Wizard. If you define a non-DMI gateway, you cannot change it to a DMI gateway later.
4	The **IP address** and **Net Mask** options are not available for a Virtual Switch.
5	**Optional:** Define a **Default Gateway** for a Virtual Router (DMI only).

Wizard Step 5: VSX Gateway Management

On the **VSX Gateway Management (Specify the management access rules)** page:

Step	Instructions
1	Examine the default access rules.
2	Select the applicable default access rules. Select **Allow** to pass traffic on the selected services. Clear the **Allow** option to block traffic on this service. By default, all services are blocked. For example, to be able to ping the VSX Gateway from the Management Server, allow ICMP Echo-Request traffic.
3	Configure the applicable source objects, if needed. Click the arrow and select a **Source Object** from the list. The default value is ***Any**. Click **New Source Object** to define a new source. You can modify the Security Policy rules that protect the VSX Gateway later.
4	Click **Next**

Important:

- This policy is installed automatically on the new VSX Gateway. These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.
  Traffic destined for Virtual Systems, other Virtual Devices, external networks, and internal networks is not affected by this policy.

This Security Policy consists of predefined rules for these services:

- **TCP** - SSH traffic and HTTPS traffic
- **UDP** - SNMP requests
- **ICMP** - Echo-Request (ping)

Wizard Step 7: Completing the VSX Wizard

On the **VSX Gateway Creation Finalization** page:

Step	Instructions
1	Click **Finish** and wait for the operation to finish. This may take several minutes to complete.
2	Click **View Report** for more information.
3	Click **Close**.

Confirming the VSX Gateway Software Configuration

To make sure that the policy was successfully installed:

Step	Instructions
1	Connect to the Security Group over SSH or serial console.
2	Log in to the Expert mode.

3	Run:
	`asg monitor -vs all`
	Example
	This example shows the output for a Dual Chassis VSX Gateway.
	Chassis 1 (Active) has 1 SGM in its Security Group.
	`----------`
	`| System Status - 64000 |`
	`----------`
	`| Up time | 22:38:58 hours |`
	`| SGMs | 1/1 |`
	`| Virtual Systems | 1 |`
	`| Version | R80.20SP (Build Number 39) |`
	`| FW Policy Date | 04Dec18 10:27 |`
	`| AMW Policy Date | 04Dec18 10:27 |`
	`----------`
	`| SGM ID Chassis 1 Chassis 2 |`
	`| ACTIVE STANDBY |`
	`----------`
	`| 1 ACTIVE ACTIVE |`
	`----------`

4	You can now add more SGMs to the Security Group. Run this command in Gaia gClish: `add smo security-group`
5	After all SGMs are in the state "`UP`" and enforce the Security Policy again, you can add Virtual Systems to the VSX Gateway in SmartConsole.

Step 5: Licensing and Registration on Scalable Chassis

Scalable Chassis have an initial 15-day evaluation license. After the evaluation license expires, you must license and register the system.

Each chassis is licensed separately.

If you have Dual Chassis system, you must install two licenses.

The license key (CK) is the chassis serial number.

The chassis serial number is printed on the chassis sticker.

You can also retrieve the chassis serial number from the CMM.

To retrieve the serial number:

Step	Instructions
1	Connect to one of the SGMs on the chassis over SSH or console.
2	Log in to the Expert mode.
3	Run: `asg_serial_info` Refer to the field **Standby Chassis serial**.

To register a Chassis:

Step	Instructions
1	Log in to the *Check Point User Center*.
2	In the applicable account, search for the chassis serial number.
3	**Generate a license based on the IP address of the SSM interface connected to your Management Server**. **Note** - Because a Chassis has one Management IP address, in Dual Chassis environments, the Active Chassis and Standby Chassis should be bound to the same IP address in the license. Generate two licenses and enter the *same* IP address in each license.
4	Install the license on the Chassis. ■ If you use the "`cplic put`" command, you must run it from the Gaia gClish, so that it applies to all SGMs. ■ Run the "`cplic put`" command twice, if you have a Dual Chassis environment.

Installing and Uninstalling a Hotfix on SGMs on Scalable Chassis

This chapter contains instructions for installing and uninstalling a Hotfix on SGMs:

Deployment	Procedure
Single Chassis	■ *"Installing a Hotfix on a Single Chassis" on page 318* ■ *"Uninstalling a Hotfix from a Single Chassis" on page 328*
Dual Chassis	■ *"Installing a Hotfix on Dual Chassis" on page 335* ■ *"Uninstalling a Hotfix from Dual Chassis" on page 343*

Installing a Hotfix on a Single Chassis

This procedure describes the Full Connectivity installation of an Offline CPUSE package on a Single Chassis.

Important Notes

- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in Security Gateway mode and VSX mode.

  In VSX mode, you must run all the commands in the context of VS0.
- If you finished a clean install on this chassis, then you can install a Jumbo Hotfix Accumulator **only** after you run the Gaia First Time Configuration Wizard.
- **Do not install the hotfix on all the SGMs at the same time.**

  If you do so with the command below, traffic stops passing through all SGMs until the hotfix is installed:

  ```
  installer install <Number of CPUSE Package> member_ids all
  ```
- In this procedure, you divide all SGMs 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 SGMs at one time.

  The other logical group(s) of the SGMs continues to handle traffic.

  Each logical group should contain the same number of SGMs - as close as possible.

  Examples:

Environment	Description
Single Chassis	• 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.
Single Chassis	• 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 from 1_4 to 1_5.

Best Practice - Perform this procedure over the serial console.

Procedure

Step 1 - Perform the preliminary steps

Step	Instructions
A	Make sure you have the applicable CPUSE offline package or the exported CPUSE package.
B	Transfer the CPUSE offline or exported package to the Chassis (into some directory, for example: `/home/admin/`).
C	Connect to the command line on the Chassis.
D	Log in to Gaia Clish.
E	Go to the Gaia gClish: `gclish`

F	Import the CPUSE package from the hard disk:
	`installer import local /<Full Path>/<Name of the CPUSE Offline Package>`
	Example:
	`[Global] SG-s01-01 > installer import local /home/admin/Check_Point_R82_Hotfix_Bundle_FULL.tar`

G	Show the imported CPUSE packages: `show installer packages imported`

Step	Instructions

H	Make sure the imported CPUSE package can be installed on this Chassis:
	`installer verify[`**`Press the Tab key`**`]`
	`installer verify <Number of CPUSE Package> member_ids all`
	Example:
	`[Global] SG-s01-01 > 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] SG-s01-01 >`

Step 2 - 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show cluster configuration image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set cluster configuration image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show cluster configuration image auto-clone state`

Step 3 - Install the Hotfix on SGMs in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the SGMs in the Logical Group "**A" through the console**. ■ Connect to one of the SGMs in the Logical Group "**B" over SSH**.

B	Go to the context of one of the SGMs in the Logical Group "A":
	`member <Member ID>`
	Example:
	`member 1_1`

C	Go to the Expert mode. `expert`

D	Set the SGMs in the Logical Group "A" to the state "DOWN":
	`cluster-cli set members-admin-state ids <SGM IDs in Group "A"> down`
	Example:
	`cluster-cli set members-admin-state ids 1_1-1_4 down`

E	Go to the Gaia gClish: `gclish`

F	Install the CPUSE package on SGMs in the Logical Group "A":
	`installer install [Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "A"`
	Example:
	`[Global] SG-s01-01> 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) **y**`

Step	Instructions
G	Go to the Expert mode. `expert`
H	Monitor the SGMs in the Logical Group "A" until they boot: `asg monitor`

Step 4 - Install the Hotfix on SGMs in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the SGMs in the Logical Group "**B**" **through the console**. ■ Connect to one of the SGMs in the Logical Group "**A**" **over SSH**.

B	Go to the context of one of the SGMs in the Logical Group "B":
	`member <Member ID>`
	Example:
	`member 1_5`

C	Go to Gaia gClish: `gclish`

D	Upgrade the SGMs in the Logical Group "B":
	`installer install[Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] SG-s01-01 > 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) y`

E	Go to the Expert mode. `expert`
F	Monitor the Security Group Members in the Logical Group "B" until they boot: `asg monitor`

Step 6 - Make sure the Hotfix is installed

Step	Instructions
A	Connect to the command line on the Security Group.
B	Go to the Expert mode. `expert`

C	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Uninstalling a Hotfix from a Single Chassis

This procedure describes the Full Connectivity uninstall of an Offline CPUSE package from a Single Chassis.

Important Notes

- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in Security Gateway mode 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 SGMs at the same time.**

  If you do so with the command below, traffic stops passing through all SGMs until the hotfix is uninstalled:

  ```
  installer uninstall <Number of CPUSE Package> member_ids all
  ```
- In this procedure, you divide all SGMs 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 uninstall the hotfix from one logical group of the SGMs at one time.

  The other logical group(s) of the SGMs continues to handle traffic.

  Each logical group should contain the same number of SGMs - as close as possible.

  Examples:

Environment	Description
Single Chassis	• 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.
Single Chassis	• 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 from 1_4 to 1_5.

Best Practice - Perform this procedure over the serial console.

Procedure

Step 1 - 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show cluster configuration image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set cluster configuration image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show cluster configuration image auto-clone state`

Step 2 - Uninstall a Hotfix from SGMs in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the SGMs in the Logical Group "**A**" **through the console**. ■ Connect to one of the SGMs in the Logical Group "**B**" **over SSH**.

B	Go to the context of one of the SGMs in the Logical Group "A":
	`member <Member ID>`
	Example:
	`member 1_1`

C	Go to the Expert mode. `expert`

D	Set the SGMs in the Logical Group "A" to the state "`DOWN`":
	`cluster-cli set members-admin-state ids <SGM IDs in Group "A"> down`
	Example:
	`cluster-cli set members-admin-state ids 1_1-1_4> down`

E	Go to the Gaia gClish: `gclish`

F	Uninstall the CPUSE package from SGMs in the Logical Group "A":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "A"`
	Example:
	`[Global] SG-s01-01 > 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`

Step	Instructions
G	Go to the Expert mode. `expert`
H	Monitor the SGMs in the Logical Group "A" until they boot: `asg monitor`

Step 3- Uninstall a Hotfix from SGMs in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the SGMs in the Logical Group "**B" through the console**. ■ Connect to one of the SGMs in the Logical Group "**A" over SSH**.

B	Go to the context of one of the SGMs in the Logical Group "B":
	`member <Member ID>`
	Example:
	`member 1_5`

C	Go to the Expert mode. `expert`

D	Set the SGMs in the Logical Group "B" to the state "DOWN":
	`cluster-cli set members-admin-state ids <SGM IDs in Group "B"> down`
	Example:
	`cluster-cli set members-admin-state ids 1_5-1_8 down`

E	Go to the Gaia gClish: `gclish`

F	Uninstall the CPUSE package from SGMs in the Logical Group "B":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "B"`
	Example:
	`[Global] SG-s01-01 > 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**`

Step	Instructions
G	Go to the Expert mode. `expert`
H	Monitor the SGMs in the Logical Group "B" until they boot: `asg monitor`

Step 4 - Make sure the Hotfix is uninstalled

Step	Instructions
A	Connect to the command line on the Security Group.
B	Go to the Expert mode. `expert`

C	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Step 5 - (Optional) Delete the uninstalled Hotfix package from the Chassis

In this **optional** step, you delete the uninstalled Hotfix package from the chassis to free the disk space.

Step	Instructions
A	Go to the Gaia gClish: `gclish`

B	Delete the uninstalled Hotfix package from the CPUSE repository on the chassis:
	`installer delete [Press the Tab key]`
	`installer delete <Number of CPUSE Package>`
	Example:
	`[Global] SG-s01-01 > installer delete 2`
	`... ...`
	`Update Service Engine`
	`+----------+----------+`
	`|Member ID |Status |`
	`+----------+----------+`
	`|1_01 (local) |Package is ready for delete |`
	`|1_02 |Package is ready for delete |`
	`|1_03 |Package is ready for delete |`
	`|1_04 |Package is ready for delete |`
	`|1_05 |Package is ready for delete |`
	`|1_06 |Package is ready for delete |`
	`|1_07 |Package is ready for delete |`
	`|1_08 |Package is ready for delete |`
	`+----------+----------+`
	`You are about to perform`
	`Package delete (Check_Point_R82_Hotfix_Bundle_FULL.tar) on blades:`
	`1_01,1_02,1_03,1_04,1_05,1_06,1_07,1_08`
	`*** In case the package is installed, you might not be able to uninstall and Import the package ever again ! ***`
	`Are you sure? (Y - yes, any other key - no) y`
	`Update Service Engine`
	`+----------+----------+`
	`|Member ID |Status |`
	`+----------+----------+`
	`|1_01 (local) |The package was successfully removed from the machine. |`
	`|1_02 |The package was successfully removed from the machine. |`
	`|1_03 |The package was successfully removed from the machine. |`
	`|1_04 |The package was successfully removed from the machine. |`
	`|1_05 |The package was successfully removed from the machine. |`
	`|1_06 |The package was successfully removed from the machine. |`
	`|1_07 |The package was successfully removed from the machine. |`
	`|1_08 |The package was successfully removed from the machine. |`
	`+----------+----------+`
	`[Global] SG-s01-01 >`

Installing a Hotfix on Dual Chassis

This procedure describes the Full Connectivity installation of an Offline CPUSE package on Dual Chassis.

Important Notes

- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in Security Gateway mode and VSX mode.

  In VSX mode, you must run all the commands in the context of VS0.
- If you finished a clean install on this chassis, then you can install a Jumbo Hotfix Accumulator only after you run the Gaia First Time Configuration Wizard.
- **Do not install the hotfix on all the SGMs at the same time.**

  If you do so with the command below, traffic stops passing through all SGMs until the hotfix is installed:

  ```
  installer install <Number of CPUSE Package> member_ids all
  ```
- In this procedure, you install the hotfix on one chassis at one time.

  The other chassis continues to handle traffic.

  1. You install the hotfix on Standby Chassis "A" from an SGM in Standby Chassis "A".
  2. You fail over all connections from Active Chassis "B" to Standby Chassis "A".
  3. You install the hotfix on Standby Chassis "B" from an SGM in Standby Chassis "B".

  In the procedures below:

  - Chassis "A" is the Standby Chassis (`chassis1`)
  - Chassis "B" is the Active Chassis (`chassis2`)

Best Practice - Perform this procedure over the serial console.

Procedure

Step 1 - Perform the preliminary steps

Step	Instructions
A	Make sure you have the applicable CPUSE offline package or the exported CPUSE package.
B	Transfer the CPUSE offline or exported package to the Chassis (into some directory, for example: `/home/admin/`).
C	Connect to the command line on **each** chassis.
D	Log in to Gaia Clish.
E	Go to the Gaia gClish: `gclish`

F	Import the CPUSE package from the hard disk:
	`installer import local /<Full Path>/<Name of the CPUSE Offline Package>`
	Example:
	`[Global] SG-s01-01 > installer import local /home/admin/Check_Point_R82_Hotfix_Bundle_FULL.tar`

G	Show the imported CPUSE packages: `show installer packages imported`

H	Make sure the imported CPUSE package can be installed on this Chassis:
	`installer verify [Press the Tab key]`
	`installer verify <Number of CPUSE Package> member_ids all`
	Example:
	`[Global] SG-s01-01 > 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.  |`
	`|2_01  |Installation is allowed.  |`
	`|2_02  |Installation is allowed.  |`
	`|2_03  |Installation is allowed.  |`
	`|2_04  |Installation is allowed.  |`
	`+----------+----------+`
	`[Global] SG-s01-01 >`

Step 2 - 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show cluster configuration image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set cluster configuration image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show cluster configuration image auto-clone state`

Step 3 - Install the Hotfix on Standby Chassis "A"

Step	Instructions
A	Connect to the command line on the Standby Chassis (in our example, Chassis "A" - `chassis1`).
B	Log in to the Expert mode.

C	Set the state of the Standby Chassis "A" to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 1 down`

D	Connect to one of the SGMs in the Standby Chassis "A": `member <Member ID>`
E	Go to the Gaia gClish: `gclish`

F	Install the CPUSE hotfix package on the Standby Chassis "A":
	`installer install [Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids chassis<ID of Standby Chassis>`
	Example:
	`[Global] SG-s01-01 > installer install 2 member_ids chassis1`
	`... ...`
	`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_01,1_02,1_03,1_04) will automatically reboot after install.`
	`Do you want to continue? ([y]es / [n]o) y`

G	Exit from Gaia gClish to the Expert mode: `exit`
H	Monitor the system until SGMs on the Standby Chassis "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

Step	Instructions

I	Set the state of the Standby Chassis "A" to "up":
	`cluster_site_admin -c <ID of Standby Chassis> up`
	Example:
	`cluster_site_admin -c 1 up`

J	Monitor the system until SGMs on the Chassis "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

K	Make sure the Hotfix is installed on all SGMs.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Step 4 - Fail over from Active Chassis "B" to Standby Chassis "A"

In this step, you fail over all connections from the Active Chassis "B" (`chassis2`) to the Standby Chassis "A" (`chassis1`).

Step	Instructions
A	Connect to the command line on the Active Chassis (in our example, Chassis "B" - `chassis2`).
B	Log in to the Expert mode.

C	Set the state of the Active Chassis "B" to "down":
	`cluster_site_admin -c <ID of Active Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

Step 5 - Install the Hotfix on Standby Chassis "B"

In this step, you install the Hotfix on all SGMs on the **former** Active Chassis "B" (`chassis2`).

Step	Instructions
A	Connect to the command line on the Standby Chassis (in our example, Standby Chassis "B" - `chassis2`).
B	Log in to the Expert mode.

C	Set the state of the Standby Chassis "B" to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

D	Connect to one of the SGMs in the Standby Chassis "B": `member <Member ID>`
E	Go to the Gaia gClish: `gclish`

F	Install the CPUSE hotfix package on the Standby Chassis "B":
	`installer install [Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids chassis<ID of Standby Chassis>`
	Example:
	`[Global] SG-s02-01 > installer install 2 member_ids chassis2`
	`... ...`
	`Update Service Engine`
	`+----------+`
	`|Member ID  |Status  |`
	`+----------+----------+`
	`|2_01 (local) |Package is ready for installation  |`
	`|2_02  |Package is ready for installation  |`
	`|2_03  |Package is ready for installation  |`
	`|2_04  |Package is ready for installation  |`
	`+----------+----------+`
	`The machines (2_01,2_02,2_03,2_04) will automatically reboot after install.`
	`Do you want to continue? ([y]es / [n]o) y`

G	Exit from Gaia gClish to the Expert mode: `exit`

Step	Instructions
H	Monitor the system until SGMs on the Standby Chassis "B" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

I	Set the state of the Standby Chassis "B" to "up":
	`cluster_site_admin -c <ID of Standby Chassis> up`
	Example:
	`cluster_site_admin -c 2 up`
	Important - If the former Active Chassis is configured as "**Primary Up**", an automatic fallback occurs.

J	Monitor the system until SGMs on the Chassis "B" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

K	Make sure the Hotfix is installed on all SGMs.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Uninstalling a Hotfix from Dual Chassis

This procedure describes the Full Connectivity uninstall of an Offline CPUSE package on Dual Chassis.

Important Notes

- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in Security Gateway mode 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 SGMs at the same time.**

  If you do so with the command below, traffic stops passing through all SGMs until the hotfix is uninstalled:

  ```
  installer uninstall <Number of CPUSE Package> member_ids all
  ```
- In this procedure, you uninstall the hotfix from one chassis at one time.

  The other chassis continues to handle traffic.

  1. You uninstall the hotfix on Standby Chassis "A" from an SGM in Standby Chassis "A".
  2. You fail over from Active Chassis "B" to Standby Chassis "A".
  3. You uninstall the hotfix on Standby Chassis "B" from an SGM in Standby Chassis "B".

  In the procedures below:

  - Chassis "A" is the Standby Chassis (`chassis1`)
  - Chassis "B" is the Active Chassis (`chassis2`)

Best Practice - Perform this procedure over the serial console.

Procedure

Step 1 - 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show cluster configuration image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set cluster configuration image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show cluster configuration image auto-clone state`

Step 2 - Uninstall the Hotfix from Standby Chassis "A"

Step	Instructions
A	Connect to the command line on the Standby Chassis (in our example, Standby Chassis A).
B	Log in to the Expert mode.

C	Set the state of the Standby Chassis "A" to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 1 down`

D	Go to the Gaia gClish: `gclish`

E	Uninstall the CPUSE hotfix package on the Standby Chassis "A":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids chassis<ID of Standby Chassis>`
	Example:
	`[Global] SG-s01-01 > installer uninstall 2 member_ids chassis1`
	`... ...`
	`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_01,1_02,1_03,1_04) will automatically reboot after uninstall.`
	`Do you want to continue? ([y]es / [n]o) y`

F	Exit from Gaia gClish to the Expert mode: `exit`
G	Monitor the system until SGMs on the Standby Chassis "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

Step	Instructions

H	Set the state of the Standby Chassis "A" to "up":
	`cluster_site_admin -c <ID of Standby Chassis> up`
	Example:
	`cluster_site_admin -c 1 up`

I	Monitor the system until SGMs on the Standby Chassis "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

J	Make sure the Hotfix is uninstalled from all SGMs.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Step 3 - Fail over from Active Chassis "B" to Standby Chassis "A"

In this step, you fail over all connections from the Active Chassis "B" (`chassis2`) to the Standby Chassis "A" (`chassis1`).

Step	Instructions
A	Connect to the command line on the Active Chassis (in our example, Standby Chassis B - (`chassis2`)).
B	Log in to the Expert mode.

C	Set the state of the Active Chassis "B" to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

Step 4 - Uninstall the Hotfix from Standby Chassis "B"

In this step, you uninstall the Hotfix from the former Standby Chassis "B" (`chassis2`).

Step	Instructions
A	Go to the Gaia gClish: `gclish`

B	Uninstall the CPUSE hotfix package on the **former** Active Chassis "B":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids chassis<ID of Standby Chassis>`
	Example:
	`[Global] SG-s01-01 > installer uninstall 2 member_ids chassis2`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------------------------+`
	`|Member ID  |Status  |`
	`+-------------+---------------------------------------------------------------+`
	`|2_01 (local) |Package is ready for uninstallation  |`
	`|2_02  |Package is ready for uninstallation  |`
	`|2_03  |Package is ready for uninstallation  |`
	`|2_04  |Package is ready for uninstallation  |`
	`+-------------+---------------------------------------------------------------+`
	`The machines (2_01,2_02,2_03,2_04) will automatically reboot after uninstall.`
	`Do you want to continue? ([y]es / [n]o) y`

C	Exit from Gaia gClish to the Expert mode: `exit`
D	Monitor the system until SGMs on the **former** Active Chassis "B" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

E	Set the state of the **former** Active Chassis "B" to "up":
	`cluster_site_admin -c <ID of Standby Chassis> up`
	Example:
	`cluster_site_admin -c 2 up`
	Important - If the former Active Chassis is configured as "**Primary Up**", an automatic fallback occurs.

Step	Instructions
F	Monitor the system until SGMs on the Chassis "B" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

G	Make sure the Hotfix is uninstalled from all SGMs.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Step 5 - (Optional) Delete the uninstalled Hotfix package from the Chassis

In this **optional** step, you delete the uninstalled Hotfix package from the chassis to free the disk space.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>A</td><td>Go to the Gaia gClish:
<pre>gclish</pre></td></tr>
<tr><td>B</td><td>Delete the uninstalled Hotfix package from the CPUSE repository on the chassis:
<pre>installer delete [Press the Tab key]
installer delete <<i>Number of CPUSE Package</i>></pre>Example:
<pre>[Global] SG-s01-01 > installer delete 2
... ...
Update Service Engine
+----------+
|Member ID |Status |
+----------+----------+
1_01 (local)	Package is ready for delete
1_02	Package is ready for delete
1_03	Package is ready for delete
1_04	Package is ready for delete
2_01	Package is ready for delete
2_02	Package is ready for delete
2_03	Package is ready for delete
2_04	Package is ready for delete
+----------+----------+
You are about to perform
Package delete (Check_Point_R82_Hotfix_Bundle_FULL.tar) on blades:
1_01,1_02,1_03,1_04,2_01,2_02,2_03,2_04
*** In case the package is installed, you might not be able to uninstall and Import
the package ever again ! ***

Are you sure? (Y - yes, any other key - no) y
Update Service Engine
+----------+
|Member ID |Status |
+----------+----------+
1_01 (local)	The package was successfully removed from the machine.
1_02	The package was successfully removed from the machine.
1_03	The package was successfully removed from the machine.
1_04	The package was successfully removed from the machine.
2_01	The package was successfully removed from the machine.
2_02	The package was successfully removed from the machine.
2_03	The package was successfully removed from the machine.
2_04	The package was successfully removed from the machine.
+----------+----------+
[Global] SG-s01-01 ></pre></td></tr>
</table>

Managing Security Groups on Scalable Chassis

This section provides basic information about managing Security Groups on Scalable Chassis.

Security Group on Scalable Chassis

To be part of a Security Gateway, a Security Gateway Module (SGM) must belong to a Security Group.

Note - On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

Viewing SGMs in a Security Group on Scalable Chassis

Syntax

```
asg stat
```

See *"asg stat" on page 829*.

Adding SGMs to a Security Group on Scalable Chassis

Best Practice - To add new SGMs to an existing Security Group:

1. Enable the SMO Image Cloning feature in the Security Group.
   This feature automatically clones all the required software packages to the new SGMs.
   Run in Gaia gClish on the Security Group:

   ```
   set cluster configuration image auto-clone state on
   ```

   ```
   show cluster configuration image auto-clone state
   ```

2. Add the new SGMs to the existing Security Group:

   ```
   add smo security-group <SGM IDs>
   ```

3. Make sure the Security Group is configured correctly (see *"insights" on page 903*):

   ```
   insights
   ```

4. To optimize connection distribution among the SGMs, update the Security Group with the correct number of the SGMs.
   See *"Configuring the SGM Range on Scalable Chassis" on page 357*.
5. Disable the SMO Image Cloning feature in the Security Group.
   Run in Gaia gClish on the Security Group:

   ```
   set cluster configuration image auto-clone state off
   ```

   ```
   show cluster configuration image auto-clone state
   ```

Syntax

```
add smo security-group <SGM IDs>
```

Parameters

Parameter	Description
<SGM IDs>	Applies to Security Group Members as specified by the *<SGM IDs>*. *<SGM IDs>* can be: ■ No *<SGM IDs>* specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

Example

```
[Global] SG-s01-01 > add smo security-group 1_1-1_3,2_1-2_3
```

Deleting SGMs from a Security Group on Scalable Chassis

Syntax

Important - Before you remove an SGM from the Security Gateway, make sure that is it in the DOWN state.
All SGMs that are assigned to the current Security Group and are not part of the new Security Group, must be in the DOWN state.
Otherwise, the command fails.

```
delete smo security-group <SGM IDs>
```

Best Practice - After you delete SGMs from an existing Security Group:

1. Make sure the Security Group is configured correctly (see *"insights" on page 903*):

   ```
   insights
   ```

2. To optimize connection distribution among the SGMs, update the Security Group with the correct number of the SGMs.
   See *"Configuring the SGM Range on Scalable Chassis" on page 357*.

Parameters

Parameter	Description
<SGM IDs>	Applies to Security Group Members as specified by the *<SGM IDs>*. *<SGM IDs>* can be: ■ No *<SGM IDs>* specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

Example

```
[Global] SG-s01-01 > delete smo security-group 1_1-1_3,2_1-2_3
```

Connecting to a Specific Security Group Member on Scalable Chassis

When you connect to the Security Group, you are actually connected to one of the Security Group Members (SGMs) in that Security Group.

You can open a connection to a different Security Group Member (SGM).

You must run the applicable command in the Expert mode, which establishes a new SSH connection over the Sync interface.

#	Syntax	Example
1	`member [<Chassis ID>_]<SGM ID>`	`[Expert@SG-s01-01:0]# member 1_03` `Moving to blade 1_3`
2	`m[<Chassis ID>_]<SGM ID>`	`[Expert@SG-s01-01:0]# m 1_03` `Moving to blade 1_3`

Notes:

- When you only enter the SGM ID, the command assumes the default Chassis.
- To go back to the previous SGM, run: `exit`
- You open many SSH sessions to SGMs.

Changing the Gaia Management Interface on Scalable Chassis

Use this command to change the Gaia management interface for the SGMs.

Important - In VSX mode, you must use the "`vsx_util change_interfaces`" command on the Management Server.

To change the Management Interface on a chassis in the Gateway mode:

Step	Instructions
1	Make sure the management interface cable is connected to the network.
2	Connect to the Scalable Chassis over a serial console. This makes sure you do not lose connectivity when you change the management interface.
3	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.

4	Run these commands in Gaia gClish in the order they are listed:
	`set management interface <New Mgmt Interface>`
	`delete interface <Current Mgmt Interface> ipv4-address`
	`set interface <New Mgmt Interface> ipv4-address <IP Address> mask-length <Length>`
	`set interface <New Mgmt Interface> state on`
	
	Parameters:
	■ *<New Mgmt Interface>*
	Interface name of the new management interface. For example: `eth1-Mgmt3`
	■ *<Current Mgmt Interface>*
	Interface name of the existing management interface that is to be changed or deleted. For example: `eth1-Mgmt2`
	■ *<IP Address>*
	Interface IPv4 address.
	■ *<Length>*
	Interface IPv4 net mask.
	
	For more information, see the *R82 Gaia Administration Guide* > Chapter *Network Management*.

Step	Instructions
5	In SmartConsole: a. Open the Security Gateway object. b. From the left tree, click **Network Management**. c. Click **Get Interfaces** > **Get Interfaces Without Topology**. d. Click **OK**. e. Install the Access Control Policy the Security Gateway object.

Configuring the SGM Range on Scalable Chassis

Description

Use the "`set blade-range`" command in Gaia gClish to configure which SGMs are part of the SGM range.

The SGM range determines on which SGMs in a Security Group to apply the Gaia gClish embedded commands you run.

Syntax

```
set blade-range <Chassis ID>_<SGM ID> - <Chassis ID>_<SGM ID>
```

Parameters

Parameter	Description
<Chassis ID>	Specifies the Chassis. Valid values: ■ `1` ■ `2`
<SGM ID>	Specifies the SGM. Valid values: ■ from `1` to `12` ■ `all` This value is not supported in the VSX mode

System Optimization on Scalable Chassis

This section describes some optimization steps you can take on Scalable Chassis.

Configuring Hyper-Threading on Scalable Chassis

Hyper-Threading mechanism runs more than one process at the same time on a CPU core.

A physical CPU that supports Hyper-Threading, adds one or more logical CPUs, which the operating system sees as independent CPUs.

Note - Hyper-Threading is enabled by default on SGM260.

To enable Hyper-Threading on Scalable Chassis:

Step	Instructions
1	Connect to the command line on the chassis.
2	Log in to Gaia Clish or the Expert mode.
3	Start the Check Point Configuration Tool: `cpconfig`
4	Select **Configure HyperThreading**.
5	Follow the on-screen instructions.
6	Reboot all SGMs: `reboot -b all`

Configuring a Dedicated Logging Port on Scalable Chassis

The Chassis logging mechanism lets each SGM forward logs directly to a dedicated Log Server over the SSM's management ports.

However, the SSM's management ports can experience a high load when SGMs generate a large number of logs.

To reduce the load on the SSM management ports:

1. Configure a dedicated SSM port for logging
2. Configure the Chassis to send the logs to the dedicated Log Server

Topology:

```
[Management Server](some interface) <===> (SSM port 1)[Chassis]

[Management Server](some interface) <===> (interface 1) [Log Server]
(interface 2) <===> (SSM port 2)[Chassis]
```

Procedure:

Step	Instructions
1	Install a dedicated Log Server: a. Install a dedicated Log Server with two physical interfaces. See the *Installation and Upgrade Guide* for your version > Chapter *Installing a Dedicated Log Server or SmartEvent Server.* b. Connect one physical interface on the dedicated Log Server to the Management Server. c. Connect another physical interface on the dedicated Log Server directly to an available SSM port. **Important** - Do **not** use the same SSM port, which connects to the Management Server. d. In SmartConsole, create the required object that represents the dedicated Log Server. See the *Installation and Upgrade Guide* for your version > Chapter *Installing a Dedicated Log Server or SmartEvent Server.*

Step	Instructions

2	In the Gaia OS of the Security Group, configure in Gaia gClish the dedicated management port on the SSM.
	Syntax:
	`[Expert@SG-s01-01:0]# gclish`
	`[Global] SG-s01-01> set interface ethX-MgmtY ipv4-address <IPv4 Address> mask-length <Mask Length>`
	Example:
	`[Global] SG-s01-01 > set interface eth1-Mgmt2 ipv4-address 2.2.2.10 mask-length 24`
	Note - You must assign an IPv4 address from the same subnet as assigned to the dedicated interface on the Log Server, which connects to the SSM.

3	In SmartConsole, configure the Security Group object to send its logs to the dedicated Log Server. See the *Logging and Monitoring Administration Guide* for your version > Chapter *Getting Started* > Section *Deploying Logging Section* - Subsection *Configuring the Security Gateways for Logging*.

Note - The SMO makes sure that return traffic from the Log Server reaches the correct Security Group Member in the Security Group.

Working with Jumbo Frames on Scalable Chassis

The Scalable Chassis 40000 / 60000 support Jumbo Frames with a total size of:

- For the SSM440 - up to 9,000 bytes
- For the SGM400 - up to 9,702 bytes

Note - Carefully calculate the MTU. For example: IPsec or GRE traffic adds bytes to the header and this leaves fewer bytes for the data payload.

Configuring Support for Jumbo Frames in a Security Group in the Gateway mode

Description

You can configure support for Jumbo Frames for each applicable interface in a Security Group.

Notes:

- This command can take several seconds to work.
- In a Dual Chassis environment, this command configures support for Jumbo Frames on both Chassis.

Syntax in Gaia gClish

```
set interface <Name of Interface> mtu <MTU Size>
```

Parameters

Parameter	Description
<Name of Interface>	Interface name as defined in the Gaia operating system.
<MTU Size>	Valid values to enable the support for Jumbo Frames: ■ For SSM440 - from 1501 to 9,000 bytes ■ For SGM400 - from 1501 to 9,702 bytes Valid values to disable the support for Jumbo Frames on all SSM and SGM models: ■ from 68 to 1500 bytes

Example 1 - Enabling Jumbo Frames on eth1-01

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > set interface eth1-01 mtu 9000
1_02:
Note: MTU changes are propagated to the SSMs. Use "asg_jumbo_
conf show" to validate changes
[Global] SG-s01-01 >
```

Example 2 - Disabling Jumbo Frames on eth1-01

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > set interface eth1-01 mtu 1500
1_02:
Note: MTU changes are propagated to the SSMs. Use "asg_jumbo_
conf show" to validate changes
[Global] SG-s01-01 >
```

Configuring Support for Jumbo Frames in a Security Group in the Traditional VSX mode

To enable the support for Jumbo Frames in a Security Group in the Traditional VSX mode:

Step	Instructions
1	Connect with SmartConsole to the Management Server that manages the Legacy VSX Gateway, or the applicable Virtual Device.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the Legacy VSX Gateway object, or the applicable Virtual Device object.
4	From the left tree, click **Topology**.
5	Edit the applicable interface.
6	On the **General** tab, set the **MTU** to 1501 or a greater value. Valid values to enable the support for Jumbo Frames: ■ For SSM440 - from 1501 to 9,0 bytes ■ For SGM400 - from 1501 to 9,702 bytes
7	Click **OK**.
8	Install Access Control Policy on the Legacy VSX Gateway object, or the applicable Virtual Device object.

To disable the support for Jumbo Frames in a Security Group in the Traditional VSX mode:

Step	Instructions
1	Connect with SmartConsole to the Management Server that manages the Legacy VSX Gateway, or the applicable Virtual Device.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the Legacy VSX Gateway object, or the applicable Virtual Device object.
4	From the left tree, click **Topology**.
5	Edit the applicable interface.
6	On the **General** tab, set the **MTU** to a value between 68 and 1500 bytes.

Step	Instructions
7	Click **OK**.
8	Install Access Control Policy on the Legacy VSX Gateway object, or the applicable Virtual Device object.

Confirming Jumbo Frames Configuration on SSM440 (asg_chassis_ctrl)

To run the validation test on the SSM:

See *"asg_chassis_ctrl" on page 1041*.

Step	Instructions
1	Show the Jumbo Frames configuration on the specified SSM: `asg_chassis_ctrl jumbo_frames show <SSM ID>`
2	Show the configured MTU on the specified SSM port: `asg_chassis_ctrl get_port_mtu <SSM ID> <Port ID>`

Example

```
[Expert@SG-s01-01:0]# asg_chassis_ctrl jumbo_frames show 1
Jumbo frames are enabled on SSM1
[Expert@SG-s01-01:0]#
```

```
[Expert@SG-s01-01:0]# asg_chassis_ctrl get_port_mtu 1 1
MTU of port 1 on SSM1 is 1544
[Expert@SG-s01-01:0]#
```

Confirming Jumbo Frames Configuration on SGMs and SGM Interfaces (asg_jumbo_conf show)

Description

You can confirm configuration of Jumbo Frames on SGMs and SGM interfaces.

Use the "`asg_jumbo_conf show`" command in the Expert mode to:

- Make sure that Jumbo Frames are enabled on the SGMs.
- See the configured MTU values on SGM interfaces configured for Jumbo Frames.

Syntax

See *"asg_jumbo_conf" on page 1057*.

```
asg_jumbo_conf show [-v]
```

Parameters

Parameter	Description
`-v`	Detailed report (verbose)

Example

```
[Expert@SG-s01-01:0]# asg_jumbo_conf show -v
Jumbo frames are enabled on SGMs (SSM1 max MTU: 12288 SSM2 max
MTU: 12288 )
Retrieving SSMs Jumbo frames configuration
Chassis1
SSMs:
Jumbo frames are enabled on SSM1
Jumbo frames are enabled on SSM2
Interfaces MTU configuration:
interface:BPEth0:mtu 12288
interface:BPEth1:mtu 12288
The MTU of all the interfaces which are not in the list is 1500
[Expert@SG-s01-01:0]#
```

Working with Rx and Tx Ring Parameters on Scalable Chassis

Use the `ethtool` command in the Expert mode to change in the size of Rx (receive) and Tx (transmit) ring parameters.

The ring parameters are also called interface buffers.

This change is supported only for the `BPEth0` and `BPEth1` interfaces.

Viewing the Current Configuration

```
ethtool -g {BPEth0 | BPEth1}
```

Example:

```
[Expert@SG-s01-01:0]# ethtool -g BPEth0
Ring parameters for BPEth0:
Pre-set maximums:
RX: 4096
RX Mini: 0
RX Jumbo: 0
TX: 4096
Current hardware settings:
RX: 256
RX Mini: 0
RX Jumbo: 0
TX: 1024
[Expert@SG-s01-01:0]#
```

Configuring the Rx (Receive) Ring Parameter

```
ethtool -G {BPEth0 | BPEth1} rx <Rx Size>
```

Example:

```
[Expert@MyChassis-s01-01:0]# ethtool -G BPEth0 rx 4096
```

Configuring the Tx (Rransmit) Ring Parameter

```
ethtool -G {BPEth0 | BPEth1} tx <Tx Size>
```

Example:

```
[Expert@MyChassis-s01-01:0]# ethtool -G BPEth0 tx 4096
```

Configuring the Rx (Receive) and Tx (Transmit) Ring Parameters

```
ethtool -G {BPEth0 | BPEth1} rx <Rx Size> tx <Tx Size>
```

Example:

```
[Expert@MyChassis-s01-01:0]# ethtool -G BPEth0 rx 4096 tx 4096
```

Configuring Link State Propagation (LSP) on Scalable Chassis

Background

You can use the Link State Propagation (LSP) to bind physical interfaces together on a Scalable Chassis. This causes all bound interfaces in an LSP Port Group to go DOWN when one of the bound interfaces goes DOWN.

After a predefined period time (default is 190 seconds), all interfaces go back to the state "`UP`".

This feature makes sure that third party devices connected to a Scalable Chassis fail over quickly, when using dynamic routing.

The Link State Propagation is disabled by default.

Configuring LSP Port Groups on Scalable Chassis

You configure LSP Port Groups in the `/etc/lsp_groups.conf` file on the Scalable Chassis.

Each line in this file defines one LSP Port Group with one or more interface groups, delimited by a comma.

An interface group has one or more interfaces, delimited by a plus sign (+).

Syntax of the configuration file

Item	Description
1	LSP Port Group (full syntax)
2	Interface Group
<*if*>	Physical Interface

Example 1

```
eth1-01+eth2-01,eth3-01+eth4-01
```

In this example, the LSP Port Group has two interface groups with two interfaces:

- Interface Group 1 contains `eth1-01` and `eth2-01`
- Interface Group 2 contains `eth3-01` and `eth4-01`

Example 2

```
eth1-02+eth1-03+eth1-04+eth1-05,eth3-02+eth4-02,eth3-03+eth4-03
```

In this example, the LSP port Group has three interface groups.

One group with four interfaces and two other groups with two interfaces each.

Adding an LSP Port Group on Scalable Chassis

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `/etc/lsp_groups.conf` file: `vi /etc/lsp_groups.conf`
4	Add one line for each LSP Port Group in the file.
5	Save the changes in the file and exit the editor.
6	Copy the file to all Security Group Members: `asg_cp2blades /etc/lsp_groups.conf`

7	Restart the LSP mechanism with these two commands:
	`asg_lsp_util disable`
	`asg_lsp_util enable`
	This step in necessary for the system to detect the change.

Deleting an LSP Port Group on Scalable Chassis

Important - If you do not use the LSP, disable it (with the "`asg_lsp_util disable`" command). Do **not** delete the configuration file, or the only LSP port group line in the file.

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `/etc/lsp_groups.conf` file: `vi /etc/lsp_groups.conf`
4	Delete the applicable LSP Port Group line from the file.
5	Save the changes in the file and exit the editor.
6	Copy the file to all Security Group Members: `asg_cp2blades /etc/lsp_groups.conf`

7	Restart the LSP mechanism with these two commands:
	`asg_lsp_util disable`
	`asg_lsp_util enable`
	This step in necessary for the system to detect the change.

Dual Chassis in Active/Standby High Availability Mode

This chapter describes how to deploy Dual Chassis in the Active/Standby High Availability mode.

How Dual Chassis Active/Standby Mode Works

Background

The Dual Chassis High Availability mechanism is based on two identical Scalable Chassis.

One Scalable Chassis handles traffic (Active state), while the other Scalable Chassis is in the Standby state.

The Standby Chassis synchronizes with the Active Chassis, so that traffic continues uninterrupted when there is a Chassis failover.

- Chassis High Availability works on the principle that the Scalable Chassis with the highest **quality grade** becomes the Active Chassis.

  To make sure that the most reliable Chassis is Active, each Chassis is assigned a quality grade.

  The quality grade is based on a continuous monitoring of Chassis critical components and traffic characteristics.

  Automatic failover occurs only when the quality grade of the Standby Chassis is greater than the quality grade of the Active Chassis, plus the minimum differential.

  A configurable minimum grade differential prevents unnecessary failover, which can cause performance degradation.

  See:

  - *"Configuring Scalable Chassis High Availability" on page 374*
  - *"Configuring the Quality Grade Differential" on page 377*
  - *"Configuring Chassis Weights (Chassis High Availability Factors)" on page 374*
- Each Chassis port has its own unique MAC address.

  The MAC addresses for SGMs are the same on the same Chassis.

  The MAC addresses are different for the ports on the two Chassis.

  A Chassis failover event sends GARP / ICMPv6 packets for each interface. This informs the network to use the other interfaces.

With the applicable Gaia gClish commands, you configure these High Availability parameters:

- Chassis High Availability - "Active Up" Mode or "Primary Up" Mode.
- Chassis quality grade factors
- Failover grade difference for failover
- Failover freeze interval
- Port priority

Configuring Dual Chassis Active/Standby Mode

Syntax

```
set cluster configuration high-availability mode <Mode ID>
```

Available Modes

Mode ID	Mode Title	Mode Description
0	**Active/Standby - Active Up**	No primary Chassis. The currently Active Chassis stays Active unless it goes DOWN, or the Standby Chassis has a higher Chassis quality grade.
1	**Active/Standby - Primary Up**	Active Chassis always stays Active unless it goes DOWN, or the Standby Chassis has a higher Chassis quality grade. See *"Configuring the Chassis Priority" on page 379*.
2	Not available	Not supported.
3	**Standby Chassis VSLS Mode**	In the Traditional VSX mode, provides Virtual System Load Sharing.

Synchronizing Dual Chassis on a Wide Area Network

You can install your Chassis at two different remote sites as a geographically distributed cluster.

There are two limitations to this capability:

1. The synchronization network must guarantee no more than 100ms latency and no more than 5% packet loss.
2. The synchronization network can include switches and hubs.

   Routers cannot be installed on the synchronization network because they drop Cluster Control Protocol packets.

Configuring Scalable Chassis High Availability

Use these settings to configure Active/Standby Chassis.

Configuring Chassis Weights (Chassis High Availability Factors)

Each hardware component in a Chassis has a quality weight factor, which sets its relative importance to overall Chassis health.

For example, ports are more important than fans and are typically assigned a higher weight value.

The Chassis grade is the sum of all component weight values.

In a High Availability environment, the Chassis with the higher grade becomes Active and handles traffic.

The grade for each component is calculated based on this formula:

```
(Unit Weight) x (Number of components in the state "UP")
```

To see the weight of each component, run in Gaia gClish:

```
asg stat -v
```

Description

Use the "`set cluster configuration high-availability factors`" command to configure a hardware component's weight.

Syntax in Gaia gClish of the Security Group

`set cluster configuration high-availability factors member <`*`SGM Factor`*`>`
`set cluster configuration high-availability factors port {other <`*`Other Port Factor`*`> | standard <`*`Standard Port Factor`*`> | mgmt <`*`Management Port Factor`*`> | bond <`*`Bond Port Factor`*`>}`
`set cluster configuration high-availability factors sensor {cmm <`*`CMM Factor`*`> | fans <`*`Fans Factor`*`> | power_supplies <`*`PSU Factor`*`> | ssm <`*`SSM Factor`*`>}`

For more information, see:

- *"show cluster configuration high-availability" on page 960*
- *"set cluster configuration high-availability" on page 925*

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.
<CMM Factor>	Weight factor for a CMM. Valid range: integer between 0 and 1000.
<Fans Factor>	Weight factor for a fan unit. Valid range: integer between 0 and 1000.
<PSU Factor>	Weight factor for a Power Supply Unit. Valid range: integer between 0 and 1000.
<SSM Factor>	Weight factor for a SSM. This factor applies to all SSMs. Valid range: integer between 0 and 1000.

Examples

```
[Global] SG-s01-01 > set cluster configuration high-availability factors sgm 100
[Global] SG-s01-01 > set cluster configuration high-availability factors port other 70
[Global] SG-s01-01 > set cluster configuration high-availability factors port standard 50
[Global] SG-s01-01 > set cluster configuration high-availability factors sensor cmm 40
[Global] SG-s01-01 > set cluster configuration high-availability factors sensor fans 30
[Global] SG-s01-01 > set cluster configuration high-availability factors sensor power_supplies 20
[Global] SG-s01-01 > set cluster configuration high-availability factors sensor ssm 45
```

Configuring the Chassis ID

You must make sure that the Chassis IDs are **different** before you start to configure the software.

Chassis IDs are configured on the CMM and should be **1** for the first Chassis and **2** for the second Chassis.

Important - If the Chassis is up and running, change the Chassis ID on the Standby Chassis. You must perform a Chassis failover.

Step	Instructions
1	Pull out the first CMM from the Chassis.
2	Connect to the remaining CMM with a serial cable (baud rate - 9600).
3	Log in with these user name and password: `admin` / `admin`
4	Edit the `/etc/shmm.cfg` file: `vi /etc/shmm.cfg`
5	Search for: `SHMM_CHASSIS=`

6	Set the correct Chassis ID:
	■ For Chassis 1:
	`SHMM_CHASSID="1"`
	■ For Chassis 2:
	`SHMM_CHASSID="2"`

7	Save the changes in the file and exit the editor.
8	Remove the current CMM and insert the second CMM.
9	Repeat Steps 2 - 6 for the second CMM.
10	Insert both CMMs into the Chassis.
11	Attach the correct identification labels to the Chassis and CMMs. This step is required if the Chassis has already been configured (after the First Time Configuration Wizard).

Step	Instructions
12	Pull out all SGMs from the Chassis. Insert all SGMs into the Chassis. **Important** - This step causes a hard reboot of the Chassis.

Configuring the Quality Grade Differential

Description

Use the "`set cluster configuration 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 cluster configuration high-availability failover <Trigger>
```

Parameters

Parameter	Description
<Trigger>	Minimum difference in Chassis quality grade to trigger a failover. Valid range: Integer between 1 and 1000.

Configuring the Failover Freeze Interval

Description

A Standby Chassis cannot failover a second time until the specified failover freeze interval expires.

The default failover freeze interval is:

- For the "Active Up" chassis configuration - 30 seconds
- For the "Primary Up" chassis configuration - 150 seconds
- For VSX Virtual System Load Sharing (VSLS) configuration - 150 seconds

If the Standby Chassis grade changes to a value greater than the minimum quality grade gap for a failover, the Standby Chassis fails over and becomes a new Active.

The failover does not start until the freeze interval expires. This confirms that the Standby Chassis quality grade is stable, before it becomes a new Active.

For example, a Standby Chassis quality grade can become unstable if a fan speed increases and decreases frequently.

Syntax in Gaia gClish of the Security Group

```
set cluster configuration high-availability freeze_interval
<Freeze Interval>
```

Parameters

Parameter	Description
<Freeze Interval>	Minimum time in seconds to wait until the next Standby Chassis failover. Valid range: integer between 1 and 1000.

Notes:

- When you run the "`asg stat`" command after Standby Chassis failover, the output shows the freeze time.
- The *<Freeze Interval>* value is 5 fold greater, if the setup is configured to work in VSLS or "Primary Up" mode.
  Example: If the freeze time must be 250 seconds, you must enter the value 50.

Configuring the Chassis Priority

After you configure the High Availability to work in the "Primary Up Mode" with the command "`set cluster configuration high-availability mode 1`" (see *"How Dual Chassis Active/Standby Mode Works" on page 371*), you must configure the chassis priority:

```
set cluster configuration high-availability vs site_priority "<ID of Primary Chassis> <ID of Secondary Chassis>"
```

Example - set Chassis 2 to be the Primary over Chassis 1:

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > set cluster configuration high-availability vs site_priority "2 1"
[Global] SG-s01-01 >
```

Advanced Dual Chassis Features

The Interface Link Preemption Mechanism in Dual Chassis

The Interface Link Preemption Mechanism prevents constant Chassis failover and fallback when the interface link state changes frequently.

When you enable this feature, an interface state that changes from DOWN to UP is included in the Chassis grade only if the link state is UP for at least "N" seconds.

The Interface Link Preemption Mechanism is enabled by default with the preemption time of 5 seconds.

Syntax to show the current configured link preemption time

Shell	Syntax
Gaia Clish	`fw ctl get int fwha_ch_if_preempt_time`
Expert mode	`g_fw ctl get int fwha_ch_if_preempt_time`

Syntax to configure the link preemption time on-the-fly (does not survive reboot)

Shell	Syntax
Gaia Clish	`fw ctl set int fwha_ch_if_preempt_time <`*`Preemption Time`*`>`
Expert mode	`g_fw ctl set int fwha_ch_if_preempt_time <`*`Preemption Time`*`>`

Syntax to configure the link preemption time permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_if_preempt_time=<`*`Preemption Time`*`>`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_if_preempt_time=<`*`Preemption Time`*`>`

Syntax to disable the link preemption mechanism on-the-fly (does not survive reboot)

Shell	Instructions
Gaia Clish	`fw ctl set int fwha_ch_if_preempt_time 0`
Expert mode	`g_fw ctl set int fwha_ch_if_preempt_time 0`

Syntax to disable the link preemption mechanism permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_if_preempt_time=0`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_if_preempt_time=0`

Parameters

Parameter	Description
<Preemption Time>	The interface link preemption time. An interface state that changes from DOWN to UP is included in the Chassis grade only if the link state is UP for at least this specified number of seconds. Default: 5 seconds

Example

```
[Expert@SG-s01-01:0]# g_fw ctl set int fwha_ch_if_preempt_time 20
[Expert@SG-s01-01:0]# g_update_conf_file fwkern.conf fwha_ch_if_
preempt_time=20
```

The Sync Lost Mechanism in Dual Chassis

The Chassis uses the Check Point proprietary Cluster Control Protocol (CCP) to send control packets between two High Availability Chassis.

When a Sync interface fails on one Chassis, it is necessary to update the other Standby Chassis.

The Sync Lost Mechanism handles the loss of connectivity between the two Chassis on the Sync network.

The Sync Lost Mechanism is enabled by default.

To prevent the two Chassis from changing their states to Active, the Chassis on which the Sync interface failed, sends the CCP packets "`sync_lost`" over the non-sync interface (the Data Ports and Management interfaces) to the other Chassis. This causes the two Chassis to freeze their current states until connectivity between the two Chassis is restored. During the Sync Loss, the Standby Chassis does not change its state to Active until it stops receiving the CCP packets "`sync_lost`" from the other Chassis.

The Chassis sends the CCP packets "`sync_lost`" in this manner:

- In a non-VSX environment - All Chassis interfaces send these CCP packets
- In a VSX environment - All interfaces of the VS0 context only send these CCP packets

Syntax to show current state of the Sync Lost Mechanism

Shell	Syntax
Gaia Clish	`fw ctl get int fwha_ch_sync_lost_mechanism_enabled`
Expert mode	`g_fw ctl get int fwha_ch_sync_lost_mechanism_enabled`

Explanation for the returned values:

- 0 - disabled
- 1 - enabled

Syntax to enable the Sync Lost Mechanism on-the-fly (does not survive reboot)

Shell	Syntax
Gaia Clish	`fw ctl set int fwha_ch_sync_lost_mechanism_enabled 1`
Expert mode	`g_fw ctl set int fwha_ch_sync_lost_mechanism_enabled 1`

Syntax to enable the Sync Lost Mechanism permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=1`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=1`

Syntax to disable the Sync Lost Mechanism on-the-fly (does not survive reboot)

Shell	Instructions
Gaia Clish	`fw ctl set int fwha_ch_sync_lost_mechanism_enabled 0`
Expert mode	`g_fw ctl set int fwha_ch_sync_lost_mechanism_enabled 0`

Syntax to disable the Sync Lost Mechanism permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=0`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=0`

Managing the Connection Synchronization in Dual Chassis

You can manage connection synchronization in Dual Chassis High Availability.

Syntax to configure the connection synchronization mode on-the-fly (does not survive reboot):

Shell	Syntax
Gaia Clish	`fw ctl set int fwha_sync_excp_mask <Mode>`
Expert mode	`g_fw ctl set int fwha_ch_sync_lost_mechanism_enabled <Mode>`

Syntax to configure the connection synchronization mode permanently (survives reboot):

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_sync_excp_mask=<Mode>` `reboot -b all`
Expert mode	`g_update_conf_file fwkern.conf fwha_sync_excp_mask=<Mode>` `g_reboot -b all`

Syntax to show the configured connection synchronization mode

```
asg stat -v
```

Parameters

Parameter	Description
<Mode>	Specifies the Connection Synchronization Mode: ■ `0` - Disables the backup synchronization on the Active Chassis and the Standby Chassis ■ `1` - Synchronizes only the backup member on the Active Chassis ■ `2` - Synchronizes only the backup member on the Standby Chassis ■ `3` - Synchronizes the backup member on the Active Chassis and the Standby Chassis

Working with SyncXL in Dual Chassis

SyncXL™ is a Check Point technology that makes sure that active connections are only synchronized to one Security Group Member (SGM) on the Active Chassis and the Standby Chassis.

When the state of an SGM or Standby Chassis changes, all SGMs update their counterpart SGMs.

These events automatically trigger the synchronization:

Event	Description
SGM Failure	Connections with a backup connection on an SGM are synchronized to a backup SGM
SGM Recovery	The newly recovered SGM can be: ■ A backup for connections that are active on other SGMs ■ Active for connections before the SGM failure
Standby Chassis High Availability Failover	When the Active Chassis fails over to the Standby Chassis, a backup entry is defined for each connection the Active Chassis handles.

Ratio between SGMs on the Standby Chassis and the Active Chassis

- To handle load and capacity, the Standby Chassis must have at least 50% of its SGMs in the state "`UP`", compared with the Active Chassis.

  For example, if there are 10 SGMs in the state "`UP`" on the Active Chassis, there must be at least 5 SGMs in the state "`UP`" on the Standby Chassis.

  SyncXL is automatically disabled if this condition is not met.

  The kernel parameter "`fwha_sync_between_chassis_blades_ratio`" controls the ratio threshold (default is 50%):

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

Step	Instructions
3	Configure the required value for the kernel parameter in the current session (does not survive reboot): `g_fw ctl set int fwha_sync_between_chassis_blades_ratio <Value>`
4	Configure the required value for the kernel parameter permanently (survives reboot): `g_update_conf_file fwkern.conf fwha_sync_between_chassis_blades_ratio=<Value>`

- Make sure that each active connection has backups on both Standby Chassis in a Dual Chassis:

  Set the value of the kernel parameter "`fwha_sync_excp_mask`" to `3` as described in *"Managing the Connection Synchronization in Dual Chassis" on page 384*.

Notes:

- VoIP connections are synchronized to all SGMs.
- Local connections (to and from the Standby Chassis's pseudo IP address) are not synchronized.
- SyncXL does not work on the Sync interface, or the Management interface.

Setting the Administratively DOWN State on First Join in Dual Chassis

Note - This section applies to Scalable Chassis.
For ElasticXL Cluster and Maestro, see *"Setting the Administratively DOWN State on First Join" on page 571*.

Description

You can configure the Scalable Chassis to set a newly installed SGM in a Security Group to be in the administratively DOWN state automatically.

The administrator can confirm that the SGM is configured correctly before changing its state to UP.

Syntax

```
set cluster configuration high-availability down_on_first_join {0
| 1}
```

- 0 - Do **not** enable the administratively DOWN state automatically on an SGM on first join
- 1 - Enable the administratively DOWN state automatically on an SGM first join

To add a new SGM to a Security Group in the administratively DOWN state

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in.
3	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`
4	Enable the administratively DOWN state automatically on a new SGM for the first join: `set cluster configuration high-availability down_on_ first_join 1` To disable, run the same command with the value 0 (zero).
5	Install a new SGM into the Chassis. See *"Adding or Replacing an SGM on Scalable Chassis" on page 490*.

Step	Instructions
6	Add the new SGM to the Security Group: `add smo security-group <SGM ID>` See *"Security Group on Scalable Chassis" on page 350*.
7	Make sure the SGM configuration is correct.
8	Change the SGM state to "UP": `set cluster members-admin-state ids <SGM ID> up` See *"set cluster members-admin-state" on page 933*.

Configuring a Unique IP Address per Site (UIPS) in Dual Chassis

In a Dual Chassis deployment:

- A heavy load on the Active Chassis can prevent you from creating a network connection to the SMO and working with management tasks.
- It can be necessary to have a direct access to the Standby Chassis to troubleshoot a problem, such as an SGM in the DOWN state.

  You cannot use the SMO to connect to the Standby Chassis.

You can assign a unique IP address to each Standby Chassis to help resolve these issues.

This adds an alias IP address to the **management interface** that is assigned to the Security Group.

When there is a high load on the SMO, connect to the Standby Chassis using the unique IP address you assigned to the Standby Chassis.

The SGMs on the Standby Chassis are always in the state "`UP`" and available to run Gaia gClish commands.

Notes:

- The UIPS feature is disabled by default on Scalable Chassis.
- The UIPS feature does not support IPv6 addresses (Known Limitation MBS-9128).
- Only one SGM runs the "UIPS" task (similar to the "SMO" task).
  In the CLI output, this task appears as "UIPC" (the former name of this feature is "Unique IP Address per Chassis").
- If the Standby Chassis is not managed through a management port, you can add the unique IP address to one of the data ports.
  The connection to the unique IP address reaches a specific SGM based on the distribution configuration.

Description

Use the "`set cluster configuration unique-ip ...`" command in Gaia gClish to assign a unique IP address to a Standby Chassis.

Important - After you assign a unique IP address to a Standby Chassis, you must make sure the Access Control policy of the Security Group allows the connection to the alias IP address.

Syntax

- *"show cluster configuration unique-ip" on page 965*
- *"set cluster configuration unique-ip" on page 931*

```
show cluster configuration unique-ip site-id <ID of Standby Chassis> interface <Name of Mgmt Interface>
```

```
set cluster configuration unique-ip <ID of Standby Chassis> interface <Name of Mgmt Interface> ipv4-address <IPv4 Address> mask-length <Length of Subnet Mask>
```

```
set cluster configuration unique-ip <ID of Standby Chassis> apply_unique_config
```

```
delete cluster configuration unique-ip site-id <ID of Standby Chassis> interface <Name of Mgmt Interface>
```

Parameters

Parameter	Description
<ID of Standby Site>	Specifies the ID of the Standby Chassis. Valid values: ■ `1` - Chassis #1 ■ `2` - Chassis #2 ■ `all` - All Chassis
<Name of Mgmt Interface>	Specifies the name of the Management Interface that is assigned to the Security Group. For example, `eth1-Mgmt1`.
<IPv4 Address>	Specifies the alias IPv4 address on the same network as one of the SGMs' interfaces.
<Length of Subnet Mask>	Specifies the length of the IPv4 subnet mask.

Example 1 - Adding a UIPS

```
[Expert@HostName-s01-01:0]# gclish
[Global] HostName-s01-01 > set cluster configuration unique-ip 1 interface eth1-Mgmt4 ipv4-
addess 172.16.6.186 mask-length 24
1_01:
Adding Alias address 172.16.6.186 of eth1-Mgmt4
1_02:
Adding Alias address 172.16.6.186 of eth1-Mgmt4
2_01:
2_02:
Alias IP was added successfully to Site 1
Alias IP address should be added to the policy rulebase in SmartDashBoard
[Global] HostName-s01-01 >
```

Example 2 - Deleting a UIPS

```
[Expert@HostName-s01-01:0]# gclish
[Global] HostName-s01-01 > delete cluster configuration unique-ip site-id 1 interface eth1-Mgmt4
1_01:
Deleting Alias IP 172.16.6.186 of eth1-Mgmt4
1_02:
Deleting Alias IP 172.16.6.186 of eth1-Mgmt4
2_01:
2_02:
Alias IP of Site 1 was deleted successfully
Alias IP address should be removed from the policy rulebase in SmartDashBoard
[Global] HostName-s01-01 >
```

Monitoring Link State of Management Interfaces in Dual Chassis

By default, Standby Chassis monitors the link state only on data ports (`eth<X>-<YZ>`).

The Management Monitor feature uses SNMP to monitor management ports for the SSM440 hardware components.

The link state is sent to all SGMs and is integrated with the Standby Chassis High Availability mechanism.

The Management Monitor feature is disabled by default.

To enable this feature, run the "`set cluster configuration high-availability mgmt-monitoring on`" command in Gaia gClish on the Security Group (see *"set cluster configuration high-availability" on page 925*).

When the Management Monitor feature is enabled:

- The monitored management ports are included in the Standby Chassis grade mechanism, according to the predefined factors (default is 11).
- The output of the "`asg stat -v`" command shows the Management ports.

  See the "`Site 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.

Important:
In a Dual Chassis deployment, if the number of SGMs differs between Standby Chassis 1 and Standby Chassis 2, after you activate the monitoring of management interfaces, you must manually adjust the gap in the chassis grade that is required for chassis failover.
The grade is calculated from all healthy modules in the system: SGM, SSM, Fans, PSU, and so on.
For example:

- Standby Chassis 1 has the grade of X
- Standby Chassis 2 has the grade of Y
- If the difference between these grades is greater than 11, chassis failover occurs

Example

```
[Expert@SG-s01-01:0]# gclish

[Global] SG-s01-01 > show cluster configuration high-availability mgmt-monitoring
1_01:
off

1_02:
off

1_03:
off

1_04:
off

1_05:
off

2_01:
off

2_02:
off

2_03:
off

2_04:
off

2_05:
off

[Global] SG-s01-01 > set cluster configuration high-availability mgmt-monitoring on
1_01:
success

1_02:
success

1_03:
success

1_04:
success

1_05:
success

2_01:
success

2_02:
success

2_03:
success

2_04:
success

2_05:
```

```
success

[Global] SG-s01-01 > asg stat -v

------------------------------------------------------------------------------
| System Status - 64000                                                      |
------------------------------------------------------------------------------
| Cluster Mode                | Active Up                                    |
| Up time                     | 2 days, 02:26:01 hours                       |
| Members                     | 10/10                                        |
| Version                     | R82 (Build Number XXX)                      |
------------------------------------------------------------------------------
| Member ID             Site1                              Site2              |
|                       STANDBY                            ACTIVE             |
------------------------------------------------------------------------------
|  1                   ACTIVE                             ACTIVE              |
|  2                   ACTIVE                             ACTIVE              |
|  3                   ACTIVE                             ACTIVE              |
|  4                   ACTIVE                             ACTIVE              |
|  5                   ACTIVE                             ACTIVE              |
------------------------------------------------------------------------------
| Site Parameters                                                            |
------------------------------------------------------------------------------
| Unit        |        Site1              |        Site2              | Weight |
------------------------------------------------------------------------------
| Members     |          5 / 5            |          5 / 5            |   6    |
| Ports       |                           |                           |        |
|   Standard  |          1 / 1            |          1 / 1            |  11    |
|   Bond      |          2 / 2            |          2 / 2            |  11    |
|   Mgmt      |          1 / 1            |          1 / 1            |  11    |
|   Mgmt Bond |          0 / 0            |          0 / 0            |  11    |
|   Other     |          0 / 0            |          0 / 0            |   6    |
| Sensors     |                           |                           |        |
|   Fans      |          6 / 6            |          6 / 6            |   5    |
|   SSMs      |          2 / 2            |          2 / 2            |  11    |
|   CMMs      |          2 / 2            |          2 / 2            |   6    |
|   PSUs      |          5 / 5            |          5 / 5            |   6    |
|             |                           |                           |        |
| Grade       |        168 / 168          |        168 / 168          |   -    |
------------------------------------------------------------------------------
| Minimum grade gap for site failover:                                  11   |
| Synchronization                                                            |
|     Sync to Active site:       Enabled                                     |
|     Sync to Standby site:      Enabled                                     |
------------------------------------------------------------------------------
| Site HA mode:                Active Up                                     |
------------------------------------------------------------------------------
[Global] SG-s01-01 >

[Global] SG-s01-01 > show interfaces
+-------------------------------------------------------------------------------------------------
-----------+
|Interfaces Data
          |
+-------------------------------------------------------------------------------------------------
-----------+
|Interface      |IPv4 Address                          |Info        |Link State
|Speed|MTU  |Duplex|
|               |MAC  Address                          |            |(site1)/(site2)     |     |
   |      |
|               |IPv6 Address (global)                 |            |                    |     |
   |      |
|               |IPv6 Address (local)                  |            |                    |     |
   |      |
+---------------+--------------------------------------+------------+--------------------+-----+-
----+------+
```

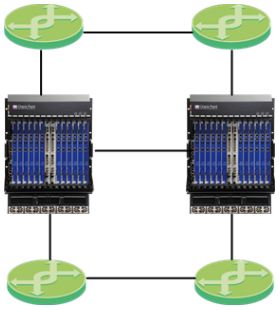
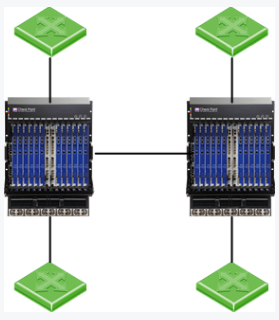
```
... ... ...
+---------------+-------------------------------------+------------+--------------------+-----+-
----+------+
|eth1-Mgmt1     |192.168.15.234/25                    |Ethernet    |(Up)/(Up)           |10G
|1500 |Full  |
|               |xx:xx:xx:xx:xx:xx                    |            |                    |     |
   |      |
|               |-                                    |            |                    |     |
   |      |
|               |xxxx::xxxx:xxxx:xxxx:xxxx/64         |            |                    |     |
   |      |
+---------------+-------------------------------------+------------+--------------------+-----+-
----+------+
... ... ...
[Global] SG-s01-01 >
```

Dual Chassis in Bridge Mode

This chapter describes how to deploy Dual Chassis in Layer 2 Bridge mode.

Bridge Mode Topologies

Active/Active Bridge Mode supports these topologies:

Topology	Description	Diagram
Layer 2 connectivity between Chassis	This topology requires Spanning Tree Protocol (STP) on the Layer 2 switches. STP is a network protocol that confirms a loop-free topology for Ethernet networks. STP sends special data frames called Bridge Protocol Data Units (BPDUs). These BPDUs help the switches select which port to block, if there is a loop detection. The BPDUs get to the switch from a different interface when they pass through the bridge interface of the chassis. This results in a successful blockage.	
No Layer 2 connectivity between Chassis	This topology does not require STP on the Layer 2 switches. It is usually a router-based topology, where a dynamic routing protocol selects through which segment to route the traffic.	

BPDU

The BDPU maximum age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information.

The default time it takes to reach a chassis failover is 20 seconds. It is possible to configure be configure this time to a value from 6 to 40 seconds.

Example for Cisco switches:

Use the "`spanning-tree vlan`" command on each VLAN to configure the BDPU maximum age timer. For more information, see Cisco documentation.

Configuring Bridge Interfaces in a Security Group in the Gateway Mode

Description

Use the applicable commands in Gaia gClish to work with Bridge interfaces.

For more information, see the *R82 Gaia Administration Guide* > Chapter *Network Management* > Section *Network Interfaces* - Subsection *Bridge Interfaces*.

Example

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > add bridging group 2
[Global] SG-s01-01 >
[Global] SG-s01-01 > add bridging group 2 interface eth2
[Global] SG-s01-01 >
[Global] SG-s01-01 > add bridging group 2 interface eth3
[Global] SG-s01-01 >
[Global] SG-s01-01 > show bridging group 2
Bridge Configuration
    Bridge Interfaces
        eth2
        eth3
[Global] SG-s01-01 >
```

Configuring Bridge Interfaces in a Security Group in the Traditional VSX Mode

Configure a Virtual System in Bridge Mode when you first create its object.

For more information, see the *R82 VSX Administration Guide*.

To configure an existing Virtual System in Active/Standby Bridge Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or the *Target*Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the Virtual System object.
4	In **Virtual System General Properties**, select **Bridge Mode**.
5	Click **Next**. The **Virtual System Network Configuration** window opens.
6	Configure the external and internal interfaces for the Virtual System.
7	Click **Next**.
8	Click **Finish**.
9	Connect to the command line on the Security Group.
10	Log in to Gaia Clish.
11	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.
12	Switch to the context of the applicable Virtual System: `set virtual-system <VS ID>`
13	Examine the interfaces: `show interfaces all`

Configuring Virtual Systems in Bridge Mode to Forward Non-IP Protocols

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Create the required empty file on all Security Group Members: `g_all touch $FWDIR/conf/enable_non_ip_protocols`
4	Follow *"Configuring Bridge Interfaces in a Security Group in the Traditional VSX Mode" on the previous page*.

Hardware Monitoring and Control on Scalable Chassis

You can monitor the hardware components on Scalable Chassis:

- *"asg_chassis_ctrl" on page 1041*
- *"asg hw_monitor" on page 1051*

Advanced Hardware Configuration on Scalable Chassis

This chapter describes advanced hardware configuration for these hardware components on Scalable Chassis:

- CMMs

  "Chassis Management Modules (CMMs) on Scalable Chassis" on page 410

- SSMs

  "Security Switch Modules (SSMs) on Scalable Chassis" on page 415

- SGMs

  "Security Gateway Modules (SGMs) on Scalable Chassis" on page 429

Configuring Port Speed on Scalable Chassis

SSM Port Speed on Scalable Chassis

SSM Ports	Port Speed
1 - 7	The port speed is can be: Auto, 1G, or 10G
8	The port speed is always 10G. This is the Sync port for Dual Chassis.
9 - 40 on SSM440	These are the QSFP ports. The port speed is according to the SSM QSFP port mode. **Note** - A license is required to use the 100GB ports on SSM440.

Supported Fanouts on SSM440:

Option	Ports 01-08	Ports 09-24	Ports 25-40
1	8 x 10G	4 x 40G	2 x 100G
2	8 x 10G	16 x 10G	2 x 100G
3	8 x 10G	4 x 40G	2 x 40G
4	8 x 10G	16 x 10G	8 x 10G

Configuring the Speed of SSM Ports 1-7 on Scalable Chassis

Description

Use these commands in Gaia gClish to configure and show the speed of the SSM data ports 1-7.

Configuration is saved to the database on all SGMs.

Syntax to configure the speed

```
set interface <Name of Port> link-speed <Speed>
```

Syntax to show the configured speed

```
show interface <Name of Port> speed
```

For more information, see the *R82 Gaia Administration Guide* > Chapter *Network Management* > Section *Network Interfaces*.

Parameters

Parameter	Description
<Name of Port>	Interface name in the "`eth<X>-<YZ>`" format. Example: `eth1-01`
<Speed>	Interface speed: ■ `auto` - Automatically selected based on the hardware detected ■ `1G` - 1 Gbit/second ■ `10G` - 10 Gbit/second

Example

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > set interface eth1-01 link-speed 1G
1_01:
success

[Global] SG-s01-01 > show interface eth1-01 speed
1_01:
speed 1G
[Global] SG-s01-01 >
```

Configuring the QSFP Port Mode for SSM Ports on Scalable Chassis

Description

Use these commands in Gaia gClish to configure and show the QSFP port mode for SSM ports.

Configuration is saved in the database on all SGMs.

Important - Changing the QSFP port mode causes the SSM to reboot. This can cause traffic outage.

Syntax

```
set ssm id <SSM ID> qsfp-ports-mode <QSFP Port Mode>
```

Note - After changing the QSFP mode on SSM ports, run the *"insights" on page 903* command and refer to the **Overview** tab to make sure the SSM ports are configured correctly.

Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><SSM ID></td><td>SSM identification number: 1 or 2.</td></tr>
<tr><td><QSFP Port Mode></td><td>Specifies the QSFP port mode and speeds.
<table>
<tr><th>SSM Model</th><th>QSFP Port Mode</th><th>Port Speeds</th></tr>
<tr><td>SSM440</td><td>2x100G_
4x40G</td><td>Ports 9, 13, 17, and 21 - work in 40G mode
Ports 25 and 33 - work in 100G mode</td></tr>
<tr><td>SSM440</td><td>6x40G</td><td>Ports 9, 13, 17, 21, 25, and 33 - work in 40G mode</td></tr>
<tr><td>SSM440</td><td>32x10G</td><td>Ports from 9 to 40 - work in 10G mode</td></tr>
<tr><td>SSM440</td><td>2x100G_
16x10G</td><td>Ports from 9 to 24 - work in 10G mode
Ports 25 and 33 - work in 100G mode</td></tr>
</table>
</td></tr>
</table>

Example for SSM440

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > set ssm id 2 qsfp-ports-mode 2x100G_16x10G
You are about to perform SSM QSFP ports mode configuration on SSM:
2 on blades: all

After this action SSM will be rebooted automatically.
It might cause performance hit or outage for a period of time.


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

SSM QSFP ports mode configuration on SSM: 2 requires auditing
Enter your full name: admin
Enter reason for SSM QSFP ports mode configuration on SSM: 2
[Maintenance]: Maintenance
WARNING: SSM QSFP ports mode configuration on SSM: 2 on blades:
all, User: admin, Reason: Maintenance
Please wait...
1_01:
success
[Global] SG-s01-01 >
```

Viewing the SSM Port Speed on Scalable Chassis

Description

Use this command in Gaia gClish to make sure that:

- The SSM port speed is configured as defined in the database.
- The SSM QSFP port mode is configured as defined in the database.

Syntax

```
show interfaces
```

Example

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > show interfaces
+-------------------------------------------------------------------------------------------------
------------+
|Interfaces Data
          |
+-------------------------------------------------------------------------------------------------
------------+
|Interface      |IPv4 Address                          |Info         |Link State
|Speed|MTU  |Duplex|
|               |MAC  Address                          |             |(site1)/(site2)     |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
|bond1          |192.168.33.212/24                     |Ethernet     |(up)/(up)           |10G
|1500 |Full  |
|               |00:1C:7F:XX:XX:XX                     |             |                    |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
|bond2          |10.33.125.212/24                      |Ethernet     |(up)/(up)           |10G
|1500 |Full  |
|               |00:1C:7F:XX:XX:XX                     |             |                    |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
|eth1-Mgmt4     |192.168.1.1/24                        |Ethernet     |(Up)/(Up)           |10G
|1500 |Full  |
|               |XX:XX:XX:XX:XX:XX                     |             |                    |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
|magg10         |192.168.15.212/25                     |Bond Master  |(up)/(up)           |20G
|NA   |Full  |
|               |XX:XX:XX:XX:XX:XX                     |             |slaves:             |     |
    |      |
|               |                                      |             |eth1-Mgmt3(Up)/(Up) |     |
    |      |
|               |                                      |             |eth2-Mgmt3(Up)/(Up) |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
|  eth1-Mgmt3   |-                                     |Bond slave   |(Up)/(Up)           |10G
|1500 |Full  |
|               |XX:XX:XX:XX:XX:XX                     |             |master:             |     |
    |      |
|               |                                      |             |magg10(up)/(up)     |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
|  eth2-Mgmt3   |-                                     |Bond slave   |(Up)/(Up)           |10G
|1500 |Full  |
|               |XX:XX:XX:XX:XX:XX                     |             |master:             |     |
    |      |
|               |                                      |             |magg10(up)/(up)     |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
|Sync           |192.0.2.15/24                         |Ethernet     |(up)/(up)           |10G
|1500 |Full  |
|               |00:1C:7F:XX:XX:XX                     |             |                    |     |
    |      |
+---------------+--------------------------------------+-------------+--------------------+-----
+-----+------+
[Global] SG-s01-01 >
```

Configuring the Management Port Speed on Scalable Chassis

Procedure

Step	Instructions
1	Connect to the command line on the SSM.

2	Run these commands in the order they are listed:
	`config`
	`port <Port Name>`
	`speed <Port Speed>`
	`commit`
	`end`

3	Make sure the port speed is correct: `show port <Port Name>`
4	Exit from the command line on the SSM: `exit`

Parameters

Parameter	Description

`<Port Name>`	Enter the applicable values:
	Interface Name / **Enter on SSM440**
	`eth<X>-Mgmt3` / `1/6/1`
	`eth<X>-Mgmt4` / `1/6/2`

`<Port Speed>`	Speed in Mbps (megabit per second). Valid values: ■ `10000` (only on SSM440) ■ `1000` ■ `100`

Chassis Management Modules (CMMs) on Scalable Chassis

Background

The Chassis Management Module (CMM) monitors and controls all hardware components in the Chassis.

The CMM communicates with a dedicated SGM using SNMP.

If a hardware sensor reports a problem, the CMM automatically takes action or sends a report.

CMMs have a Command Line Interface.

For more information, see the *Scalable Chassis Getting Started Guide* and sk93332.

Connecting to the Active CMM

Method	Instructions
Telnet, or SSH	1. Open a Telnet or SSH session from one of the SGMs. 2. Log in to the Expert mode. 3. Connect to the CMM with this command: `member CMM` 4. Enter `admin` for the user name and password.
Serial port	1. Connect to the serial port on the front panel of the CMM. 2. Open a console window in your terminal emulation program (for example, PuTTY, SecureCRT). Use the default serial connection parameters: 9600, 8, N, 1 3. Enter `admin` for the user name and password.

Connecting to the Standby CMM

Step	Instructions
1	Connect to the command line on the Active CMM (see *"Connecting to the Active CMM" on the previous page*).
2	At the command prompt, run: `ifconfig`
3	Record the IP Address for the USB interface.
4	Open a Telnet or SSH session from the Active CMM to the Standby CMM with the IP address from the table below:

IP address of Active CMM	IP address of Standby CMM
192.168.1.130	192.168.1.131
192.168.1.131	192.168.1.130
192.168.1.2	192.168.1.3
192.168.1.3	192.168.1.2

Collecting the CMM Diagnostic Information (clia fruinfo)

Step	Instructions
1	Connect to the command line on the Active CMM (see *"Connecting to the Active CMM" on the previous page*).
2	Configure your terminal emulation program (for example, PuTTY, SecureCRT) to save the log file for the current session.
3	Get the contents of the `/etc/summary` file: `cat /etc/summary` **Note** - This command can take several minutes to run.
4	Get the contents of the `/tmp/debug.log` file: `cat /tmp/debug.log`
5	Get the contents of the `/etc/shmm.cfg` file: `cat /etc/shmm.cfg`

Step	Instructions

6	Run these commands to collect the hardware information:
	`clia fruinfo 20 0`
	`clia fruinfo 20 1`
	`clia fruinfo 20 2`
	`clia fruinfo 20 3`
	`clia fruinfo 20 4`
	`clia fruinfo 20 5`
	`clia fruinfo 20 6`
	`clia fruinfo 20 7`
	`clia fruinfo 20 8`
	`clia fruinfo 20 9`

Step	Instructions

7	Run these commands to collect the hardware information:
	`clia fruinfo y 10`
	`clia fruinfo y 12`
	`clia fruinfo y 82`
	`clia fruinfo y 84`
	`clia fruinfo y 86`
	`clia fruinfo y 88`
	`clia fruinfo y 8a`
	`clia fruinfo y 8c`
	`clia fruinfo y 8e`
	`clia fruinfo y 90`
	`clia fruinfo y 92`
	`clia fruinfo y 94`
	`clia fruinfo y 96`
	`clia fruinfo y 98`
	`clia fruinfo y 9a`
	`clia fruinfo y 9c`

8	Get the contents of the `/tmp/debug.log` file again: `cat /tmp/debug.log`

Changing the CMM Administrator Password

Step	Instructions
1	Connect to the command line on the CMM.
2	Log in to the Expert mode.
3	Change the password: `passwd admin`
4	Enter and confirm the new password.

Changing the Chassis Configuration

To change the Chassis configuration, edit this file:

```
/etc/shmm.cfg
```

CMM Commands

Command	Syntax	Description
`clia help`	`clia help`	Shows a list of available commands.
`clia alarm`	`clia alarm [0]`	Shows and resets the current alarms on the CMM.
`clia board`	`clia board`	Confirms the boards are recognized.
`clia fru`	`clia fru <SGM ID>` `clia fru <SSM ID>`	Shows information about an SGM or SSM.
`clia reboot`	`clia reboot`	Reboots the CMM. The Chassis fails over to the Standby CMM.
`clia sel`	`clia sel`	Retrieves event logs.
`clia shelf pd`	`clia shelf pd`	Shows power consumption information for all boards.
`ic2 test`	`ic2_test`	■ Tests the I2C connection ■ Detects all devices connected to the CMM using I2C

Security Switch Modules (SSMs) on Scalable Chassis

The Security Switch Module (SSM):

- Distributes network traffic to the Security Gateway Modules (SGMs)
- Transmits traffic to and from the SGMs
- Shares the load between the SGMs

The SSMs and SGMs communicate automatically through SNMP requests. You can also connect directly to the SSM and run CLI commands.

The SSM contains two modules:

- **Fabric switch** - Includes the data ports
- **Base switch** - Includes the management ports

For more information, see the *Scalable Chassis Getting Started Guide* and sk93332.

SSM CLI

The SSM communicates with the SGMs through SNMP.

Sometimes, it is necessary to connect directly to the SSM and run CLI commands.

Connecting to the SSM CLI

You can connect to the SSM CLI in one of these ways:

Connection	Description
Through a serial console port on the SSM front panel	Use the default serial connection parameters: 9600, 8, N, 1

From the CLI of one of the SGMs	1. Connect to the command line on the SGM.
	2. Log in to the Expert mode.
	3. Go to the CLI on the applicable SSM:
	`member ssm1`
	`member ssm2`

Important - The default administrator password for the SSM CLI is: `admin`

Available SSM CLI Commands

Command	Description
`show running-config [<Feature Name>]`	Shows the current SSM configuration. **Best Practice** - Because the full configuration is very long, we recommended that you show a configuration only for one specified feature. To see a full list of the available features, enter "`show running-config`" and press the **Tab** key. For example, run the "`show running-config load-balance`" command to see the load balancing configuration.
`show port`	Shows the current status of SSM ports.
`show port <Port ID>`	Shows detailed port information such as speed, administrative state, link state and so on for the specified SSM port.
`show port <Port ID> statistics`	Shows interface statistics for the specified SSM port.
`show version`	Shows the firmware version.

Example

```
[Global] SG-s01-01:0> show port 1/3/1 statistics
================================================================================
 Port Statistics
================================================================================
                                                 Input                  Output
--------------------------------------------------------------------------------
Unicast Packets                                   5003                    7106
Multicast Packets                               568409                    1880
Broadcast Packets                               122151                    1972
Flow Control                                         0                       0
Discards                                            16                       0
Errors                                               0                       0
--------------------------------------------------------------------------------
Total                                           695563                   10958
================================================================================

================================================================================
 Ethernet Statistics in Packets
================================================================================
RX CRC Errors                     0         TX Collisions                     0
RX Undersize                      0
--------------------------------------------------------------------------------
                                                 Input                  Output
--------------------------------------------------------------------------------
Fragments                                            0                       0
Oversize                                             0                       0
Jabbers                                              0                       0
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Packets                                                       Input and Output
--------------------------------------------------------------------------------
Octets                                                                71085491
Packets                                                                 706521
Packets of 64 Octets                                                      2290
Packets of 65 to 127 Octets                                             689951
Packets of 128 to 255 Octets                                              4122
Packets of 256 to 511 Octets                                              6009
Packets of 512 to 1023 Octets                                              258
Packets of 1024 to 1518 Octets                                             994
Packets of 1519 or more Octets                                               0
--------------------------------------------------------------------------------
Total                                           695563                   10958
================================================================================

================================================================================
 Rates in Bytes per Second
================================================================================
                                                 Input                  Output
Rate for last 10 sec                              1477                      25
Rate for last 60 sec                              1435                      50
================================================================================
[Global] SG-s01-01:0>
```

Note - In the output of this specific command, pay special intention to the **Discards** and **Errors** fields. If the values in these fields constantly increase, this can indicate a problem.

Viewing the SSM Logs

Step	Instructions
1	Connect to the command line on the SSM. See *"Connecting to the SSM CLI" on page 415*.
2	Enable the private shell: `unhide private` The default password is: `private`
3	Open the private shell: `show private shell`
4	Run: `tail /var/log/messages`

Changing the Load Distribution on SGM Groups

Step	Instructions
1	Connect to the command line on the SSM. See *"Connecting to the SSM CLI" on page 415*.
2	Connect to the configuration terminal: `configure terminal`
3	Configure the load distribution on SGM Groups: `(config)# load-balance mtx-bucket 1 buckets [<SGM ID1><SGM ID2>:<SGM ID3><SGM ID4> ...]` **Important** - You must provide a full list of the SGMs. Otherwise, SSM might drop the traffic.
4	Save the changes: `(config)# commit`
5	Exit the configuration terminal: `(config)# exit`
6	Apply the new load distribution configuration: `load-balance apply`
7	Log out from current session: `logout`

Changing the SSM Administrator Password

Note - You must perform this procedure on each SSM separately. This procedure does not cause any traffic interruption.

Step	Instructions
1	Connect to an SGM over SSH or serial console.
2	Log in to the Expert mode.

3	Go to one of the SSMs:
	`member ssm1`
	`member ssm2`

4	Enter the administrator password. The default administrator password for the SSM CLI is: `admin`
5	Connect to the configuration terminal: `configure terminal`
6	Configure the administrator user: `system security user admin`
7	Configure the password: `password`
8	Enter the new password.
9	Save the changes: `(config)# commit`
10	End the current session: `end`
11	Log out from current session: `logout`

Example

```
[Expert@SG-s01-01:0]# member ssm2
Moving to ssm2
T-ATCA404
admin@ssm2's password: *****
BATM T-ATCA404
admin connected from 198.51.100.204 using ssh on T-ATCA404
--- WARNING ---------------------------------------------------------
Running db may be inconsistent. Enter private configuration mode and
install a saved configuration.
---------------------------------------------------------------------
T-ATCA404#
T-ATCA404# conf t
Entering configuration mode terminal
T-ATCA404 (config)# system security user admin
T-ATCA404 (config-user-admin)# password
(<MD5 digest string>): *****
T-ATCA404 (config-user-admin)# commit
Commit complete.
T-ATCA404 (config-user-admin)# end
T-ATCA404# logout
Connection to ssm2 closed
```

Mapping of SSM Port IDs to SGM Port IDs

Each port ID on the SGM maps to a port on the SSM.

SGM Port Mapped to SSM #1	SGM Port Mapped to SSM #2	SSM440 Port
eth1-01	eth2-01	1/1/1
eth1-02	eth2-02	1/1/2
eth1-03	eth2-03	1/1/3
eth1-04	eth2-04	1/1/4
eth1-05	eth2-05	1/1/5
eth1-06	eth2-06	1/1/6
eth1-07	eth2-07	1/1/7
eth1-Sync	eth2-Sync	1/1/8
eth1-09	eth2-09	1/4/1
eth1-10	eth2-10	1/4/2
eth1-11	eth2-11	1/4/3
eth1-12	eth2-12	1/4/4
eth1-13	eth2-13	1/4/5
eth1-14	eth2-14	1/4/6
eth1-15	eth2-15	1/4/7
eth1-16	eth2-16	1/4/8
eth1-17	eth2-17	1/4/9
eth1-18	eth2-18	1/4/10
eth1-19	eth2-19	1/4/11
eth1-20	eth2-20	1/4/12
eth1-21	eth2-21	1/4/13
eth1-22	eth2-22	1/4/14

SGM Port Mapped to SSM #1	SGM Port Mapped to SSM #2	SSM440 Port
eth1-23	eth2-23	1/4/15
eth1-24	eth2-24	1/4/16
eth1-25	eth2-25	1/2/1
eth1-26	eth2-26	1/2/2
eth1-27	eth2-27	1/2/3
eth1-28	eth2-28	1/2/4
eth1-29	eth2-29	1/2/5
eth1-30	eth2-30	1/2/6
eth1-31	eth2-31	1/2/7
eth1-32	eth2-32	1/2/8
eth1-33	eth2-33	1/3/1
eth1-34	eth2-34	1/3/2
eth1-35	eth2-35	1/3/3
eth1-36	eth2-36	1/3/4
eth1-37	eth2-37	1/3/5
eth1-38	eth2-38	1/3/6
eth1-39	eth2-39	1/3/7
eth1-40	eth2-40	1/3/8
eth1-Mgmt1	eth2-Mgmt1	N/A
eth1-Mgmt2	eth2-Mgmt2	N/A
eth1-Mgmt3	eth2-Mgmt3	1/6/1
eth1-Mgmt4	eth2-Mgmt4	1/6/2

Checking the Connectivity from the SGMs to the SSMs

Step	Instructions
1	Connect to the command line on an SGM.
2	Log in to the Expert mode.
3	Send ping from SGMs to IP addresses of all the SSMs.
4	Get the firmware version of all SSMs: `asg_chassis_ctrl get_ssm_firmware all`

Adding or Removing SSMs After Initial Setup

Description

If you add or remove SSMs after the initial chassis installation, the chassis can show an incorrect number of installed SSMs or an SSM in the DOWN state.

Use the "`asg_ssm_amount`" command to define the correct number of SSMs in the chassis.

Important:

- When you change the number of SSMs, it is necessary to reboot the chassis. This interrupts the traffic.
- You must run this command if you add or remove SSMs on the Standby Chassis.
- Make sure that only one SGM is turned on when you run this command.
- When you change the number of SSMs from 2 to 1, make sure that the remaining SSM is installed in the SSM Slot 1.

Syntax

```
asg_ssm_amount <Number of SSMs in Standby Chassis>
```

Parameters

Parameter	Description
<Number of SSMs in Standby Chassis>	Total number of SSMs in the Standby Chassis. For more information, see the *Scalable Chassis Getting Started Guide* > Chapter *Hardware Components*.

Changing the number of SSMs

You can change the number of SSMs with one of these procedures.

Procedure 1 - Requires a long down time

This procedure is for changing the number of SSMs from 1 to 2.

This procedure is simple, but requires a longer down time, because you reboot all SGMs at the same time.

Step	Instructions
1	Make sure all SGMs are in the state "`UP`".
2	Connect to the SMO Security Group Member over a serial console. Using a console connection, in the Expert mode, run on the SMO:
3	Log in to the Expert mode.
4	Set the number of SSMs in the Standby Chassis to two: `asg_ssm_amount 2`
5	Reboot all SGMs: `reboot -b all`
6	Wait for all the SGMs to be in the state "`UP`". **Note** - An additional reboot is expected. The utility prompts you for auto-reboot.
7	Insert the new SSM. Use a console connection to monitor the booting process. **Note** - In a Dual Chassis configuration, make sure to connect the new sync slave.
8	On the SMO Security Group Member, run: `asg_port_speed create_conf`

9	Verify the configuration integrity.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Procedure 2 - Requires a minimal down time, but requires to disconnect the Sync and Data ports

This procedure is for changing the number of SSMs from 1 to 2, and from 2 to 1.

This procedure requires a minimal down time, because the Standby Chassis are rebooted one at a time.

However, this procedure requires to disconnect the Sync and Data ports, which causes a traffic outage.

Part 1 - On the Standby Chassis

Step	Operation	Command	Notes
1	Disconnect the cables from the Sync and Data ports on the Standby Chassis.		
2	Physically pull out all the SGMs except the SMO.		
3	Physically install or remove the additional SSMs. **Important** - When you change the number of SSMs from 2 to 1, make sure that the remaining SSM is installed in the SSM Slot 1.		
4	Using a console cable, connect to the remaining SGM (SMO).		

Step	Operation	Command	Notes

5	Configure the required number of SSMs.	■ To set the number of SSMs to one:
		`asg_ssm_amount 1`
		■ To set the number of SSMs to two:
		`asg_ssm_amount 2`	

6	Reboot the remaining SGM (SMO).	`reboot`	

7	When the SGM is in the state "`UP`" on the Standby Chassis, make sure the configuration matches the configured number of SSMs.	a. Examine the list of active SSMs:
		`ccutil active_ssm`
		Example output:
		`SSM1 ACTIVE`
		`SSM2 ACTIVE`
		`SSM3 ACTIVE`
		`SSM4 ACTIVE`
		b. Examine the chassis status:
		`asg stat -v`
		c. Examine the interfaces:
		`ifconfig`
			For verification, see *"Configuring the Chassis ID" on page 376*.
			Make sure the chassis has the `eth3-<XX>` and `eth4-<XX>` ports.

8	Insert all other SGMs.		
9	When the SGMs are in the state "`UP`" on the Standby Chassis, disconnect the cables from the Sync and Data ports on the Active Chassis.		This causes a traffic outage.

Step	Operation	Command	Notes
10	Connect the cables to the Sync and Data ports on the Standby Chassis.		The Standby Chassis is now the Active Chassis and inspects the traffic.

Part 2 - On the former Active Chassis

Step	Operation	Command	Notes
11	Repeat steps 2 - 8 on the former Active Chassis, which is now disconnected.		
12	Connect the cables to the Sync and Data ports on the former Active Chassis.		

13	When the SGM is in the state "`UP`" on the former Active Chassis, make sure the configuration matches the configured number of SSMs.	a. Examine the list of active SSMs:
		`ccutil active_ssm`
		Example output:
		`SSM1 ACTIVE`
		`SSM2 ACTIVE`
		`SSM3 ACTIVE`
		`SSM4 ACTIVE`
		b. Examine the chassis status:
		`asg stat -v`
		c. Examine the interfaces:
		`ifconfig`	

Security Gateway Modules (SGMs) on Scalable Chassis

Background

The Security Gateway Modules (SGMs) in the Chassis work together as a single, high performance Security Gateway or VSX Gateway. You can add SGMs and it scales the performance of the system. An SGM can be added and removed without losing connections. If an SGM is removed or fails, traffic is distributed to the other active SGMs.

These SGM models are available:

- SGM400
- SGM260
- SGM220

For more information, see the *Scalable Chassis Getting Started Guide* and sk93332.

Identifying SGMs in the Chassis (asg_detection)

Description

Use this command in the Expert mode to flash the LEDs of an SGM.

Use Case

This lets you identify the specified SGM.

Syntax

```
asg_detection [ -b <SGM IDs> ] [ -t <time> | off ]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`) The default is the local SGM, on which you run this command.
`-t <Time>`	Specifies for how long (in seconds) the LEDs flash. Default is 60 seconds.
`-t off`	Stops LED flashes if they continue after the time specified with the "`-t <Time>`" parameter.

Slot IDs for SGMs and SSMs on Scalable Chassis

Some commands use SGM IDs and SSM IDs, or Slot IPMB Addresses.

Use these tables to find the correct SGM ID and SSM ID, or Slot IPMB Address.

For additional information, see the *Scalable Chassis Getting Started Guide* > Chapter *Hardware Components*.

64000 Chassis

Physical Slot Number	Slot IPMB Address	SGM Number	SSM Number
1	0x9A	SGM1	
2	0x96	SGM2	
3	0x92	SGM3	
4	0x8E	SGM4	
5	0x8A	SGM5	
6	0x86	SGM6	
7	0x82		SSM1
8	0x84		SSM2
9	0x88	SGM7	
10	0x8C	SGM8	
11	0x90	SGM9	
12	0x94	SGM10	
13	0x98	SGM11	
14	0x9C	SGM12	

44000 Chassis

Physical Slot Number	Slot IPMB Address	SGM Number	SSM Number
1	0x82		SSM1
2	0x84	SGM6 (or SSM2)	SSM2 (or SGM6)

Physical Slot Number	Slot IPMB Address	SGM Number	SSM Number
3	0x86	SGM5	
4	0x88	SGM4	
5	0x8A	SGM3	
6	0x8C	SGM2	
7	0x8E	SGM1	

Upgrading Hardware Components on Scalable Chassis

This section describes the procedures for:

- *"Upgrading the CMM Firmware on N+1 Scalable Chassis" on page 434*
- *"Upgrading the CMM Firmware on N+N Scalable Chassis - CMM700" on page 442*
- *"Upgrading the CMM Firmware on N+N Scalable Chassis - CMM500" on page 466*
- *"Upgrading SSM Firmware on Scalable Chassis" on page 481*
- *"Replacing SSM160 with SSM440 on Scalable Chassis" on page 482*

Important - Firmware packages are provided in sk161293.

Upgrading the CMM Firmware on N+1 Scalable Chassis

It is possible to upgrade or downgrade a CMM firmware version.

Important:

- The procedure below applies only to **CMM500**.
- Firmware packages are provided in sk161293.
- In a Dual Chassis configuration, all CMMs must have the same firmware version.
  1. Upgrade the CMM Firmware on the Standby Chassis
  2. Fail over from the Active Chassis to the Standby Chassis
  3. Upgrade the CMM Firmware on the former Active Chassis
- At certain points during this procedure, the CMM functionality is interrupted. At these times, hardware monitoring data is not collected and the chassis fans rotate at maximum speed.

Notes:

- When the command includes the "`-c`" parameter, enter the Standby Chassis ID number only, not the word "`chassis`".
  For example: `cluster_site_admin -c 1 down`
- When the command includes the "`-b`" parameter, enter the word "`chassis`" and after it enter the Standby Chassis ID number.
  For example: `g_reboot -a -b chassis1`

Best Practice - We recommend that you manually enter the commands below. Because of the command syntax is long, a mistake can occur if you copy and paste it. Incorrect syntax can causes an unexpected behavior.

Part 1 - Upgrading the CMM Firmware on the Standby Chassis

In this part, you upgrade the CMM firmware on the Standby Chassis.

Procedure

Step	Operation	Command
1	Connect to the command line on the Standby Chassis.	
2	Log in to the Expert mode.	
3	Set the state of the Standby Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`

Step	Operation	Command
4	Connect to the command line on an SGM on the Standby Chassis. Connect SSH or a serial console.	
5	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
6	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM_update.tar -C /var/log/`
7	Pull out all CMMs on the Standby Chassis.	
8	Insert one CMM into the Standby Chassis.	
9	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm500.* admin@198.51.100.33:/tmp/`
10	Open a console connection to the serial port on the CMM's front panel. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	

Step	Operation	Command
11	Make sure the system health is normal. This confirms that all upgrade files and sentry files were successfully copied to the CMM.	`# clia shelf info_force_update` `# ls /tmp`

12	Copy the CMM firmware image.	`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

13	Run the firmware installation script. When prompted, press Enter to reboot the CMM. **Note** - If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`

14	Follow the instructions on the screen.
	When prompted, select the applicable chassis parameters.
	For more information about the PSU type, see sk91980.
	Note- The screens that appear can be slightly different than appears on the right.
		`Select one of following options.`
		`1: Press 1 for AC1(Telkoor) or DC.`
		`2: Press 2 for AC2(Lambda).`
		`3: Press 3 for DC power records.`
		`Power records Modification`
		`1: Press 1 for AC power records.`
		`2: Press 2 for DC power records.`
		`3: Press 3 to skip.`
		`EEprom upgrading`
		`1: Press 1 for EEProm upgrading.`
		`2: Press 2 to skip.`

Step	Operation	Command
15	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
16	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
17	To upgrade the second CMM: a. Pull out the first upgraded CMM b. Insert the second CMM c. Repeat Steps 1 - 16	
18	Insert the first upgraded CMM.	
19	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	
20	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
21	Set the state of the Standby Chassis to Admin UP.	`cluster_site_admin -c <`*`ID of Standby Chassis`*`> up`

Part 2 - Failing Over from Active Chassis to Standby Chassis

In this part, you fail over all connections from the Active Chassis to the Standby Chassis.

Procedure

Step	Instructions
22	Connect to the command line on the Active Chassis.
23	Log in to the Expert mode.

24	Set the state of the Active Chassis to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

Part 3 - Upgrading the CMM Firmware on the former Active Chassis

In this part, you upgrade the CMM firmware on the former Active Chassis.

Procedure

Step	Operation	Command
25	Connect to the command line on the former Active Chassis.	
26	Log in to the Expert mode.	
27	Set the state of the former Active Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`
28	Connect to the command line on an SGM on the former Active Chassis. Connect SSH or a serial console.	

Step	Operation	Command
29	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
30	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM_update.tar -C /var/log/`
31	Pull out all CMMs on the former Active Chassis.	
32	Insert one CMM into the former Active Chassis.	
33	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm500.* admin@198.51.100.33:/tmp/`
34	Open a console connection to the serial port on the CMM's front panel. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	
35	Make sure the system health is normal. This confirms that all upgrade files and sentry files were successfully copied to the CMM.	`# clia shelf info_force_update` `# ls /tmp`

Step	Operation	Command

36	Copy the CMM firmware image.	`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

37	Run the firmware installation script.	`install.sh`

38	Follow the instructions on the screen.
	When prompted, select the applicable chassis parameters.
	For more information about the PSU type, see sk91980.
	Note- The screens that appear can be slightly different than appears on the right.
		`Select one of following options.`
		`1: Press 1 for AC1(Telkoor) or DC.`
		`2: Press 2 for AC2(Lambda).`
		`3: Press 3 for DC power records.`
		`Power records Modification`
		`1: Press 1 for AC power records.`
		`2: Press 2 for DC power records.`
		`3: Press 3 to skip.`
		`EEprom upgrading`
		`1: Press 1 for EEProm upgrading.`
		`2: Press 2 to skip.`

39	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
40	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`

Step	Operation	Command
41	To upgrade the second CMM: a. Pull out the first upgraded CMM b. Insert the second CMM c. Repeat Steps 25 - 40	
42	Insert the first upgraded CMM.	
43	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	
44	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
45	Set the state of the former Active Chassis to Admin UP. **Important** - If the former Active Chassis is configured as "**Primary Up**", an automatic fallback occurs.	`cluster_site_admin -c <ID of Standby Chassis> up`

Upgrading the CMM Firmware on N+N Scalable Chassis - CMM700

It is possible to upgrade or downgrade a CMM firmware version.

Important:

- The procedures below apply only to **CMM700**.
- Firmware packages are provided in sk161293.
- In a Dual Chassis configuration, all CMMs must have the same firmware version.
  1. Upgrade the CMM Firmware on the Standby Chassis
  2. Fail over from the Active Chassis to the Standby Chassis
  3. Upgrade the CMM Firmware on the former Active Chassis
- At certain points during these procedures, the CMM functionality is interrupted. At these times, hardware monitoring data is not collected and the chassis fans rotate at maximum speed.

Notes:

- When the command includes the "`-c`" parameter, enter the Standby Chassis ID number only, not the word "`chassis`".
  For example: `cluster_site_admin -c 1 down`
- When the command includes the "`-b`" parameter, enter the word "`chassis`" and after it enter the Standby Chassis ID number.
  For example: `g_reboot -a -b chassis1`

Best Practice - We recommend that you manually enter the commands below. Because of the command syntax is long, a mistake can occur if you copy and paste it. Incorrect syntax can causes an unexpected behavior.

Upgrading the CMM Firmware on CMM700 - With Physical Access to Standby Chassis

Use this procedure if there is a physical access to the chassis.

All the required steps were divided into three parts.

Part 1 - Upgrading the CMM Firmware on the Standby Chassis

In this part, you upgrade the CMM firmware on the Standby Chassis.

Procedure

Step	Operation	Command
1	Connect to the command line on the Standby Chassis.	

Step	Operation	Command
2	Log in to the Expert mode.	
3	Set the state of the Standby Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`
4	Connect to the command line on an SGM on the Standby Chassis. Connect over SSH or a serial console.	
5	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
6	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM700CC_update.tar -C /var/log/`
7	Pull out all CMMs from the Standby Chassis.	
8	Insert one CMM into the Standby Chassis.	
9	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm700.* admin@198.51.100.33:/tmp/`
10	Open a console connection to the serial port on the CMM on the Standby Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	

Step	Operation	Command

11	Copy the CMM firmware image to the CMM.
	Note - Run these commands from the console connection to the CMM.
		`cd /tmp`
		`clia terminate`
		`setenv custcnf C00013`
		`setenv rc2 /etc/rc.0000-14`
		`rupgrade --erase-all --base file:///tmp/sentry.shmm700. -k kernel -r rfs -a app`

12	Run the firmware installation script. **Notes:** ▪ Run this command from the console connection to the CMM. ▪ When prompted, press Enter to reboot the CMM. ▪ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`
13	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
14	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`

Step	Operation	Command
15	Pull out the upgraded CMM from the Standby Chassis.	
16	Insert the second CMM into the Standby Chassis.	
17	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm700.* admin@198.51.100.33:/tmp/`
18	Open a console connection to the serial port on the CMM on the Standby Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	

19	Copy the CMM firmware image to the CMM.
	Note - Run these commands from the console connection to the CMM.
		`cd /tmp`
		`clia terminate`
		`setenv custcnf C00013`
		`setenv rc2 /etc/rc.0000-14`
		`rupgrade --erase-all --base file:///tmp/sentry.shmm700. -k kernel -r rfs -a app`

Step	Operation	Command
20	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`
21	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
22	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
23	Insert the first CMM into the Standby Chassis.	
24	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	

Step	Operation	Command
25	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
26	Set the state of the Standby Chassis to Admin UP.	`cluster_site_admin -c <ID of Standby Chassis> up`

Part 2 - Failing Over from Active Chassis to Standby Chassis

In this part, you fail over all connections from the Active Chassis to the Standby Chassis.

Procedure

Step	Instructions
27	Connect to the command line on the Active Chassis.
28	Log in to the Expert mode.

29	Set the state of the Active Chassis to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

Part 3 - Upgrading the CMM Firmware on the former Active Chassis

In this part, you upgrade the CMM firmware on the former Active Chassis.

Procedure

Step	Operation	Command
30	Connect to the command line on the former Active Chassis.	
31	Log in to the Expert mode.	
32	Set the state of the former Active Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`

Step	Operation	Command
33	Connect to the command line on an SGM on the former Active Chassis. Connect over SSH or a serial console.	
34	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
35	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM700CC_update.tar -C /var/log/`
36	Pull out all CMMs from the former Active Chassis.	
37	Insert one CMM into the former Active Chassis.	
38	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm700.* admin@198.51.100.33:/tmp/`
39	Open a console connection to the serial port on the CMM on the former Active Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	

Step	Operation	Command

40	Copy the CMM firmware image to the CMM.
	Note - Run these commands from the console connection to the CMM.
		`cd /tmp`
		`clia terminate`
		`setenv custcnf C00013`
		`setenv rc2 /etc/rc.0000-14`
		`rupgrade --erase-all --base file:///tmp/sentry.shmm700. -k kernel -r rfs -a app`

41	Run the firmware installation script. **Notes:** ▪ Run this command from the console connection to the CMM. ▪ When prompted, press Enter to reboot the CMM. ▪ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`
42	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
43	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`

Step	Operation	Command
44	Pull out the upgraded CMM from the former Active Chassis.	
45	Insert the second CMM into the former Active Chassis.	
46	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm700.* admin@198.51.100.33:/tmp/`
47	Open a console connection to the serial port on the CMM on the former Active Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	

48	Copy the CMM firmware image to the CMM.
	Note - Run these commands from the console connection to the CMM.
		`cd /tmp`
		`clia terminate`
		`setenv custcnf C00013`
		`setenv rc2 /etc/rc.0000-14`
		`rupgrade --erase-all --base file:///tmp/sentry.shmm700. -k kernel -r rfs -a app`

Step	Operation	Command
49	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`
50	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
51	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
52	Insert the first CMM into the former Active Chassis.	
53	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	

Step	Operation	Command
54	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
55	Set the state of the former Active Chassis to Admin UP. **Important** - If the former Active Chassis is configured as "**Primary Up**", an automatic fallback occurs.	`cluster_site_admin -c <ID of Standby Chassis> up`

Upgrading the CMM Firmware on CMM700 - No Physical Access to Standby Chassis

Use this procedure if there is **no** physical access to the chassis.

This procedure requires a console connection to each CMM.

All the required steps were divided into three parts.

Part 1 - Upgrading the CMM Firmware on the Standby Chassis

In this part, you upgrade the CMM firmware on the Standby Chassis.

Procedure

Step	Operation	Command
1	Connect to the command line on the Standby Chassis.	
2	Log in to the Expert mode.	
3	Set the state of the Standby Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`
4	Open a console connection to the serial port on the Active CMM and on the Standby CMM on the Standby Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	
5	Connect to the command line on an SGM on the Standby Chassis. Connect over SSH or a serial console.	

Step	Operation	Command
6	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
7	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM700CC_update.tar -C /var/log/`
8	Terminate the Standby CMM on the Standby Chassis.	a. Identify the Standby CMM: `clia shmstatus` b. From the console connection to the Standby CMM, terminate the CMM: `clia terminate`
9	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm700.* admin@198.51.100.33:/tmp/`

Step	Operation	Command

10	Copy the CMM firmware image to the Active CMM.
	Notes:
	■ Run these commands from the console connection to the Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`clia terminate`
		`setenv custcnf C00013`
		`setenv rc2 /etc/rc.0000-14`
		`rupgrade --erase-all --base file:///tmp/sentry.shmm700. -k kernel -r rfs -a app`

11	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`

Step	Operation	Command
12	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
13	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`

14	Terminate the Active CMM on the Standby Chassis.
	Run these commands from the console connection to Active CMM.
		a. Terminate the CMM:
		`clia terminate`
		b. Set the state of the `eth0` interface to down:
		`ifconfig eth0 down`
		c. Set the state of the `eth1` interface to down:
		`ifconfig eth1 down`

15	Reboot the Standby CMM. **Notes:** ■ Run this command from the console connection to the Standby CMM: ■ This CMM becomes the new Active CMM.	`reboot`

16	Terminate the Standby CMM (former Active CMM) on the Standby Chassis.	a. Identify the Standby CMM:
		`clia shmstatus`
		b. From the console connection to the Standby CMM (former Active CMM), terminate the CMM:
		`clia terminate`

Step	Operation	Command
17	Copy the firmware files from the SGM to the `/tmp/` directory on the new Active CMM (former Standby CMM). The password is: `admin`	`# scp /var/log/sentry.shmm500.* admin@198.51.100.33:/tmp/`

18	Copy the CMM firmware image to the new Active CMM.
	Notes:
	■ Run these commands from the console connection to the new Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

Step	Operation	Command
19	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the new Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`
20	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
21	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
22	Reboot the Standby CMM. Run this command from the console connection to the Standby CMM:	`reboot`
23	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	

Step	Operation	Command
24	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
25	Set the state of the Standby Chassis to Admin UP.	`cluster_site_admin -c <ID of Standby Chassis> up`

Part 2 - Failing Over from Active Chassis to Standby Chassis

In this part, you fail over all connections from the Active Chassis to the Standby Chassis.

Procedure

Step	Instructions
26	Connect to the command line on the Active Chassis.
27	Log in to the Expert mode.

28	Set the state of the Active Chassis to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

Part 3 - Upgrading the CMM Firmware on the former Active Chassis

In this part, you upgrade the CMM firmware on the former Active Chassis.

Procedure

Step	Operation	Command
29	Connect to the command line on the former Active Chassis.	
30	Log in to the Expert mode.	
31	Set the state of the former Active Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`

Step	Operation	Command
32	Open a console connection to the serial port on the Active CMM and on the Standby CMM on the former Active Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	
33	Connect to the command line on an SGM on the former Active Chassis. Connect over SSH or a serial console.	
34	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
35	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM700CC_update.tar -C /var/log/`
36	Terminate the Standby CMM on the former Active Chassis.	a. Identify the Standby CMM: `clia shmstatus` b. From the console connection to the Standby CMM, terminate the CMM: `clia terminate`
37	Copy the firmware files from the SGM to the `/tmp/` directory on the CMM. The password is: `admin`	`# scp /var/log/sentry.shmm700.* admin@198.51.100.33:/tmp/`

Step	Operation	Command

38	Copy the CMM firmware image to the Active CMM.
	Notes:
	■ Run these commands from the console connection to the Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`clia terminate`
		`setenv custcnf C00013`
		`setenv rc2 /etc/rc.0000-14`
		`rupgrade --erase-all --base file:///tmp/sentry.shmm700. -k kernel -r rfs -a app`

39	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`

Step	Operation	Command
40	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
41	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
42	Terminate the Active CMM on the former Active Chassis. Run these commands from the console connection to Active CMM.	a. Terminate the CMM: `clia terminate` b. Set the state of the `eth0` interface to down: `ifconfig eth0 down` c. Set the state of the `eth1` interface to down: `ifconfig eth1 down`
43	Reboot the Standby CMM. **Notes:** ■ Run this command from the console connection to the Standby CMM: ■ This CMM becomes the new Active CMM.	`reboot`
44	Terminate the Standby CMM (former Active CMM) on the former Active Chassis.	a. Identify the Standby CMM: `clia shmstatus` b. From the console connection to the Standby CMM (former Active CMM), terminate the CMM: `clia terminate`

Step	Operation	Command
45	Copy the firmware files from the SGM to the `/tmp/` directory on the new Active CMM (former Standby CMM). The password is: `admin`	`# scp /var/log/sentry.shmm500.* admin@198.51.100.33:/tmp/`

46	Copy the CMM firmware image to the new Active CMM.
	Notes:
	■ Run these commands from the console connection to the new Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

Step	Operation	Command
47	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the new Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`
48	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
49	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
50	Reboot the Standby CMM. Run this command from the console connection to the Standby CMM:	`reboot`
51	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	

Step	Operation	Command
52	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
53	Set the state of the former Active Chassis to Admin UP. **Important** - If the former Active Chassis is configured as "**Primary Up**", an automatic fallback occurs.	`cluster_site_admin -c <ID of Standby Chassis> up`

Upgrading the CMM Firmware on N+N Scalable Chassis - CMM500

It is possible to upgrade or downgrade a CMM firmware version.

Important - The procedure below applies only to **CMM500**.
Use this procedure if there is **no** physical access to the chassis.
This procedure requires a console connection to each CMM.

Important:

- Firmware packages are provided in sk161293.
- In a Dual Chassis configuration, all CMMs must have the same firmware version.
  1. Upgrade the CMM Firmware on the Standby Chassis
  2. Fail over from the Active Chassis to the Standby Chassis
  3. Upgrade the CMM Firmware on the former Active Chassis
- At certain points during this procedure, the CMM functionality is interrupted.
  At these times, hardware monitoring data is not collected and the chassis fans rotate at maximum speed.

Notes:

- When the command includes the "`-c`" parameter, enter the Standby Chassis ID number only, not the word "`chassis`".
  For example: `cluster_site_admin -c 1 down`
- When the command includes the "`-b`" parameter, enter the word "`chassis`" and after it enter the Standby Chassis ID number.
  For example: `g_reboot -a -b chassis1`

Best Practice - We recommend that you manually enter the commands below.
Because of the command syntax is long, a mistake can occur if you copy and paste it.
Incorrect syntax can causes an unexpected behavior.

All the required steps were divided into three parts.

Part 1 - Upgrading the CMM Firmware on the Standby Chassis

In this part, you upgrade the CMM firmware on the Standby Chassis.

Procedure

Step	Operation	Command
1	Open a console connection to the serial port on the Active CMM and on the Standby CMM on the Standby Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	
2	Connect to the command line on the Standby Chassis.	
3	Log in to the Expert mode.	
4	Set the state of the Standby Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`
5	Connect to the command line on an SGM on the Standby Chassis. Connect over SSH or a serial console.	
6	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
7	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM_update.tar -C /var/log/`
8	Terminate the Standby CMM on the Standby Chassis.	a. Identify the Standby CMM: `clia shmstatus` b. From the console connection to the Standby CMM, terminate the CMM: `clia terminate`

Step	Operation	Command
9	Copy the firmware files from the SGM to the `/tmp/` directory on the Active CMM. The password is: `admin`	`# scp /var/log/sentry.shmm500.* admin@198.51.100.33:/tmp/`

10	Copy the CMM firmware image to the Active CMM.
	Notes:
	■ Run these commands from the console connection to the Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

Step	Operation	Command
11	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`

12	Follow the instructions on the screen.
	When prompted, select the applicable chassis parameters.
	For more information about the PSU type, see sk91980.
	Note- The screens that appear can be slightly different than appears on the right.
		`Select one of following options.`
		`1: Press 1 for AC1(Telkoor) or DC.`
		`2: Press 2 for AC2(Lambda).`
		`3: Press 3 for DC power records.`
		`Power records Modification`
		`1: Press 1 for AC power records.`
		`2: Press 2 for DC power records.`
		`3: Press 3 to skip.`
		`EEprom upgrading`
		`1: Press 1 for EEProm upgrading.`
		`2: Press 2 to skip.`

13	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`

Step	Operation	Command
14	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`

15	Terminate the Active CMM on the Standby Chassis.
	Run these commands from the console connection to Active CMM.
		a. Terminate the CMM:
		`clia terminate`
		b. Set the state of the `eth0` interface to down:
		`ifconfig eth0 down`
		c. Set the state of the `eth1` interface to down:
		`ifconfig eth1 down`

16	Reboot the Standby CMM. **Notes:** ■ Run this command from the console connection to the Standby CMM: ■ This CMM becomes the new Active CMM.	`reboot`

17	Terminate the Standby CMM (former Active CMM) on the Standby Chassis.	a. Identify the Standby CMM:
		`clia shmstatus`
		b. From the console connection to the Standby CMM (former Active CMM), terminate the CMM:
		`clia terminate`

18	Copy the firmware files from the SGM to the `/tmp/` directory on the new Active CMM (former Standby CMM). The password is: `admin`	`# scp /var/log/sentry.shmm500.*` `admin@198.51.100.33:/tmp/`

Step	Operation	Command

19	Copy the CMM firmware image to the new Active CMM.
	Notes:
	■ Run these commands from the console connection to the new Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

20	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the new Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`

Step	Operation	Command

21	Follow the instructions on the screen.
	When prompted, select the applicable chassis parameters.
	For more information about the PSU type, see sk91980.
	Note- The screens that appear can be slightly different than appears on the right.
		`Select one of following options.`
		`1: Press 1 for AC1(Telkoor) or DC.`
		`2: Press 2 for AC2(Lambda).`
		`3: Press 3 for DC power records.`
		`Power records Modification`
		`1: Press 1 for AC power records.`
		`2: Press 2 for DC power records.`
		`3: Press 3 to skip.`
		`EEprom upgrading`
		`1: Press 1 for EEProm upgrading.`
		`2: Press 2 to skip.`

22	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
23	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
24	Reboot the Standby CMM. Run this command from the console connection to the Standby CMM:	`reboot`

Step	Operation	Command
25	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	
26	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
27	Set the state of the Standby Chassis to Admin UP.	`cluster_site_admin -c <ID of Standby Chassis> up`

Part 2 - Failing Over from Active Chassis to the Standby Chassis

In this part, you fail over all connections from the Active Chassis to the Standby Chassis.

Procedure

Step	Instructions
28	Connect to the command line on the Active Chassis.
29	Log in to the Expert mode.

30	Set the state of the Active Chassis to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

Part 3 - Upgrading the CMM Firmware on the former Active Chassis

In this part, you upgrade the CMM firmware on the former Active Chassis.

Procedure

Step	Operation	Command
31	Open a console connection to the serial port on the Active CMM and on the Standby CMM on the former Active Chassis. Use the default connection parameters: ■ Baud Rate: 9600 ■ Data bits: 8 ■ Stop bits: 1 ■ Parity: None ■ Flow Control: None	
32	Connect to the command line on the former Active Chassis.	
33	Log in to the Expert mode.	
34	Set the state of the former Active Chassis to Admin DOWN.	`cluster_site_admin -c <ID of Standby Chassis> down`
35	Connect to the command line on an SGM on the former Active Chassis. Connect over SSH or a serial console.	
36	Get the applicable firmware version. Usually the latest recommended firmware file is located here: `$SMODIR/conf/hw_firmware/SM_update.tar`	
37	Extract the firmware image on the SGM to the `/var/log/` directory.	`tar -xvf $SMODIR/conf/hw_firmware/SM_update.tar -C /var/log/`
38	Terminate the Standby CMM on the former Active Chassis.	a. Identify the Standby CMM: `clia shmstatus` b. From the console connection to the Standby CMM, terminate the CMM: `clia terminate`

Step	Operation	Command
39	Copy the firmware files from the SGM to the `/tmp/` directory on the Active CMM. The password is: `admin`	`# scp /var/log/sentry.shmm500.* admin@198.51.100.33:/tmp/`

40	Copy the CMM firmware image to the Active CMM.
	Notes:
	■ Run these commands from the console connection to the Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

Step	Operation	Command
41	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`

42	Follow the instructions on the screen.
	When prompted, select the applicable chassis parameters.
	For more information about the PSU type, see sk91980.
	Note- The screens that appear can be slightly different than appears on the right.
		`Select one of following options.`
		`1: Press 1 for AC1(Telkoor) or DC.`
		`2: Press 2 for AC2(Lambda).`
		`3: Press 3 for DC power records.`
		`Power records Modification`
		`1: Press 1 for AC power records.`
		`2: Press 2 for DC power records.`
		`3: Press 3 to skip.`
		`EEprom upgrading`
		`1: Press 1 for EEProm upgrading.`
		`2: Press 2 to skip.`

43	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`

Step	Operation	Command
44	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
45	Terminate the Active CMM on the former Active Chassis. Run these commands from the console connection to Active CMM.	a. Terminate the CMM: `clia terminate` b. Set the state of the `eth0` interface to down: `ifconfig eth0 down` c. Set the state of the `eth1` interface to down: `ifconfig eth1 down`
46	Reboot the Standby CMM. **Notes:** ■ Run this command from the console connection to the Standby CMM: ■ This CMM becomes the new Active CMM.	`reboot`
47	Terminate the Standby CMM (former Active CMM) on the former Active Chassis.	a. Identify the Standby CMM: `clia shmstatus` b. From the console connection to the Standby CMM (former Active CMM), terminate the CMM: `clia terminate`
48	Copy the firmware files from the SGM to the `/tmp/` directory on the new Active CMM (former Standby CMM). The password is: `admin`	`# scp /var/log/sentry.shmm500.* admin@198.51.100.33:/tmp/`

Step	Operation	Command

49	Copy the CMM firmware image to the new Active CMM.
	Notes:
	■ Run these commands from the console connection to the new Active CMM.
	■ After the CMM reboot, these lines appear. Press Enter to get the login prompt:
	`<INFO> Write confirmed: 1 -> 0 [ALLOW]`
	`<INFO> Write upgrade_state: "in progress" (2) -> "confirmed" (4) [ALLOW]`
	`<INFO> Write upgrade watchdog: 1 -> 0 [ALLOW]`
		`cd /tmp`
		`setenv rc2 /etc/rc.asis`
		`clia terminate`
		`rupgrade_tool -s -v --r=sentry.shmm500.rfs --k=sentry.shmm500.kernel --u=sentry.shmm500.u-boot --hook=erase`

50	Run the firmware installation script. **Notes:** ■ Run this command from the console connection to the new Active CMM. ■ When prompted, press Enter to reboot the CMM. ■ If the screen becomes unreadable during the upgrade procedure, change the baud rate of the console connection.	`install.sh`

Step	Operation	Command

51	Follow the instructions on the screen.
	When prompted, select the applicable chassis parameters.
	For more information about the PSU type, see sk91980.
	Note- The screens that appear can be slightly different than appears on the right.
		`Select one of following options.`
		`1: Press 1 for AC1(Telkoor) or DC.`
		`2: Press 2 for AC2(Lambda).`
		`3: Press 3 for DC power records.`
		`Power records Modification`
		`1: Press 1 for AC power records.`
		`2: Press 2 for DC power records.`
		`3: Press 3 to skip.`
		`EEprom upgrading`
		`1: Press 1 for EEProm upgrading.`
		`2: Press 2 to skip.`

52	If the Standby Chassis ID is 2, change the Standby Chassis ID setting from "1" to "2".	`sed -i 's/CHASSID="1"/CHASSID="2"/g' /etc/shmm.cfg` `reboot`
53	Make sure the Standby Chassis ID is correct. Outputs of the commands listed on the right must be the same and must show the correct Standby Chassis ID. **Important** - If outputs of these commands do **not** match, stop the entire procedure and contact *Check Point Support* immediately.	`grep SHMM_CHASSID /etc/shmm.cfg` `clia shelfaddress`
54	Reboot the Standby CMM. Run this command from the console connection to the Standby CMM:	`reboot`

Step	Operation	Command
55	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.	
56	Make sure the Active and Standby CMMs have the same firmware version.	`asg_version -i`
57	Set the state of the former Active Chassis to Admin UP. **Important** - If the former Active Chassis is configured as "**Primary Up**", an automatic fallback occurs.	`cluster_site_admin -c <ID of Standby Chassis> up`

Upgrading SSM Firmware on Scalable Chassis

Important - Firmware packages are provided in sk161293.

Use the "`asg_ssm_upgrade`" utility in the Expert mode to upgrade the SSM firmware to the most recent version.

Upgrade one SSM at a time.

Syntax:

```
asg_ssm_upgrade ssm <SSM ID> [chassis <Chassis ID>] [file
<Firmware File>]
```

Parameters

Parameter	Description
<SSM ID>	Specifies the SSM ID to upgrade. Valid values: ■ 1 ■ 2 ■ all
<Chassis ID>	Specifies the Chassis ID. Valid values: ■ 1 ■ 2 ■ all
<Firmware File>	Specifies the absolute path and name of the new firmware file.

Important:

- Before you upgrade, confirm that the checksum of the new firmware file is valid.
- You must copy the new firmware file to all SGMs.
- You must connect over console when upgrade the SSM firmware on the chassis.
  In Dual Chassis, this does not applies if you upgrade the SSM firmware on the other chassis.
- The SSM automatically reboots after the upgrade. This can cause traffic interruption.

Replacing SSM160 with SSM440 on Scalable Chassis

Important - Interfaces **eth<N>-Mgmt1** and **eth<N>-Mgmt2** are no longer available.

See sk101556 for specific commands.

To support 40 BP speed with SGM400, see sk118435.

Replacing SSM160 with SSM440 on a Single Chassis

Procedure

Step	Instructions
1	Connect over a serial console the Chassis.
2	Connect to the command line on the Chassis over SSH.

3	Get the diagnostics data before the upgrade.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`
	Save the output from the screen.

4	If necessary, add licenses for 100G.
5	Set the state of the Chassis to "down": `cluster_site_admin -c 1 down`
6	Shut down all SSMs on the Chassis.

7	Shut down all SGMs on the Chassis from the Expert mode.
	`gexec -b chassis1 -a -c "shutdown -h now"`
	`gexec -r -a -c "shutdown -h now"`

8	Pull out all SGMs from the Chassis: a. Loosen the thumb screws at the top and bottom of the SGM. b. Open the latches at the top and bottom of the SGM. c. Partially slide out the SGM.

Step	Instructions
9	Pull out all **SSM160** from the Chassis.
10	Insert all **SSM440** into the Chassis.
11	Wait about 2 minutes. Over a serial console connection, check that the port links are up on the SSMs: `asg_chassis_ctrl get_ports_link <SSM ID>`
12	Insert all SGMs on the Chassis.
13	When the SGMs are in the state "`UP`", reboot the SGMs (because of the SSM change). Reboot each SGM by partially sliding it out and immediately pushing it back in place: a. Loosen the thumb screws at the top and bottom of the SGM. b. Open the latches at the top and bottom of the SGM. c. Partially slide out the SGM. d. Push back the SGM. e. Fasten the latches. f. Tighten the thumb screws.
14	Set the state of the Chassis to "up": `cluster_site_admin -c 1 up`

15	Get the diagnostics data again.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`
	Save the output from the screen.
	Compare the new data with the data you collected before you replaced the SSMs.

Replacing SSM160 with SSM440 on Dual Chassis

All the required steps were divided into three parts.

Part 1 - Replacing SSM160 with SSM440 on the Chassis

In this part, you replace all SSM160 with SSM440 on the Standby Chassis.

Procedure

Step	Instructions
1	Connect over a serial console the Standby Chassis.
2	Connect to the command line on the Standby Chassis over SSH.

3	Get the diagnostics data before the upgrade.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`
	Save the output from the screen.

4	If necessary, add licenses for 100G.

5	Set the state of the Standby Chassis to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 1 down`

6	Shut down all SSMs on the Standby Chassis.

7	Shut down all SGMs on the Standby Chassis from the Expert mode.
	`gexec -b chassis<ID of Standby Chassis> -a -c "shutdown -h now"`
	`gexec -r -a -c "shutdown -h now"`

8	Pull out all SGMs from the Standby Chassis: a. Loosen the thumb screws at the top and bottom of the SGM. b. Open the latches at the top and bottom of the SGM. c. Partially slide out the SGM.

Step	Instructions
9	Pull out all **SSM160** from the Standby Chassis.
10	Insert all **SSM440** into the Standby Chassis.
11	Wait about 2 minutes. Over a serial console connection, check that the port links are up on the SSMs: `asg_chassis_ctrl get_ports_link <SSM ID>`
12	Insert all SGMs on the Standby Chassis.
13	When the SGMs are in the state "`UP`", reboot the SGMs (because of the SSM change). Reboot each SGM by partially sliding it out and immediately pushing it back in place: a. Loosen the thumb screws at the top and bottom of the SGM. b. Open the latches at the top and bottom of the SGM. c. Partially slide out the SGM. d. Push back the SGM. e. Fasten the latches. f. Tighten the thumb screws.

14	On each SSM on the Standby Chassis, configure the same QSFP Mode as you configured on the SSMs of the Active Chassis.
	a. Connect to the command line on an SGM on the Active Chassis over SSH.
	b. Log in to the Expert mode.
	c. Get the QSFP mode:
	`asg_chassis_ctrl get_qsfp_ports_mode <SSM ID>`
	d. Connect to the command line on an SGM on the Standby Chassis over SSH.
	e. Log in to the Expert mode.
	f. Set the QSFP mode:
	Note - Do this step on one SSM at a time.
	`asg_chassis_ctrl set_qsfp_ports_mode <SSM ID>`
	g. The SSM reboots.
	Note - If there are speed changes on ports 1 - 7 on SSM440, the SSM reboots to align the configuration with the Active Chassis.

Step	Instructions

15	Set the state of the former Active Chassis to "up":
	`cluster_site_admin -c <ID of Standby Chassis> up`
	Example:
	`cluster_site_admin -c 2 up`
	Important - If the former Active Chassis is configured as "**Primary Up**", an automatic fallback occurs.

16	Get the diagnostics data again.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`
	Save the output from the screen.
	Compare the new data with the data you collected before you replaced the SSMs.

Part 2 - Failing Over from the Active Chassis to the Standby Chassis

In this part, you fail over all connections from the Active Chassis to the Standby Chassis.

Procedure

Step	Instructions
17	Connect to the command line on the Active Chassis over SSH.
18	Log in to the Expert mode.

19	Set the state of the Active Chassis to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

Part 3 - Replacing SSM160 with SSM440 on the former Active Chassis

In this part, you replace all SSM160 with SSM440 on the former Active Chassis.

Procedure

Step	Instructions
20	Connect over a serial console the former Active Chassis.
21	Connect to the command line on the former Active Chassis over SSH.

22	Get the diagnostics data before the upgrade.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`
	Save the output from the screen.

23	If necessary, add licenses for 100G.

24	Set the state of the former Active Chassis to "down":
	`cluster_site_admin -c <ID of Standby Chassis> down`
	Example:
	`cluster_site_admin -c 2 down`

25	Shut down all SSMs on the former Active Chassis.

26	Shut down all SGMs on the former Active Chassis from the Expert mode.
	`gexec -b chassis<ID of Standby Chassis> -a -c "shutdown -h now"`
	`gexec -r -a -c "shutdown -h now"`

27	Pull out all SGMs from the former Active Chassis: a. Loosen the thumb screws at the top and bottom of the SGM. b. Open the latches at the top and bottom of the SGM. c. Partially slide out the SGM.
28	Pull out all **SSM160** from the former Active Chassis.
29	Insert all **SSM440** into the former Active Chassis.

Step	Instructions
30	Wait about 2 minutes. Over a serial console connection, check that the port links are up on the SSMs: `asg_chassis_ctrl get_ports_link <SSM ID>`
31	Insert all SGMs on the former Active Chassis.
32	When the SGMs are in the state "`UP`", reboot the SGMs (because of the SSM change). Reboot each SGM by partially sliding it out and immediately pushing it back in place: a. Loosen the thumb screws at the top and bottom of the SGM. b. Open the latches at the top and bottom of the SGM. c. Partially slide out the SGM. d. Push back the SGM. e. Fasten the latches. f. Tighten the thumb screws.

33	On each SSM on the former Active Chassis, configure the same QSFP Mode as you configured on the SSMs of former Standby Chassis.
	a. Connect to the command line on an SGM on the former Standby Chassis over SSH.
	b. Log in to the Expert mode.
	c. Get the QSFP mode:
	`asg_chassis_ctrl get_qsfp_ports_mode <SSM ID>`
	d. Connect to the command line on an SGM on the former Active Chassis over SSH.
	e. Log in to the Expert mode.
	f. Set the QSFP mode:
	Note - Do this step on one SSM at a time.
	`asg_chassis_ctrl set_qsfp_ports_mode <SSM ID>`
	g. The SSM reboots.
	Note - If there are speed changes on ports 1 - 7 on SSM440, the SSM reboots to align the configuration with the current Active Chassis.

34	Set the state of the former Active Chassis to "up":
	`cluster_site_admin -c <ID of Standby Chassis> up`
	Example:
	`cluster_site_admin -c 2 up`

Step	Instructions

35	Get the diagnostics data again.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`
	Save the output from the screen.
	Compare the new data with the data you collected before you replaced the SSMs.
	Note - These tests might fail:
	a. When you run the "`asg_port_speed verify`" command from the Active Chassis (with SSM160), all tests should pass except for the QSFP Mode.
	b. When you run the "`asg_port_speed verify`" command from the Standby Chassis (with SSM440), all tests should pass except for the QSFP Mode and ports 17 - 40 (the Active Chassis should show "`N/A`").
	c. The configuration file test fails because of differences in the Gaia configuration database file (`/config/active`) - the SSM type, number of ports, speed of ports, and the QSFP Mode.
	d. SSM QoS test fails because of different port IDs between the two chassis.
	After you replace the SSM160 on the Active Chassis, the SSM QoS works again.
	e. The MAC setting test fails when you run it from the chassis with SSM440.
	The MAC setting test fails on ports 17 - 40 when you run it from the chassis with SSM160.

Replacing Hardware Components on Scalable Chassis

This chapter provides instructions for replacing these hardware components on Scalable Chassis:

- Chassis Management Module (CMM)
- Security Gateway Module (SGM)

Adding or Replacing an SGM on Scalable Chassis

In This Section:

Using Snapshot Image to Add a New or a Replacement SGM *490*

Installing a New SGM Using a CD/DVD Device *499*

You can perform an operating system upgrade on a new or replacement SGM.

There are two methods to update operating system versions:

- Create a snapshot image from one of the SGMs on the Standby Chassis and revert the new SGM to this snapshot.
- Install from a distribution media (a CD/DVD, or a USB device).

Using Snapshot Image to Add a New or a Replacement SGM

Use snapshot as a backup. Confirm that the latest hotfixes are installed on a new or replacement SGM (or if an SGM is sent for service as an RMA).

Part 1- Required steps on the working SGM

Best Practice - In a Dual Chassis configuration, create a snapshot on one of the SGMs on the Standby Chassis.

Step	Procedure	Instructions	Notes
1	Connect to the command line on the Standby Chassis, over an SSH or console connection.		

Step	Procedure	Instructions	Notes
2	Log in to the Expert mode.	`expert`	
3	Go to one of the SGMs on the Standby Chassis.	`[Expert@SG-s<ID>-<ID>:0]# member <ID of Standby Chassis>_<SGM ID>`	Example: `[Expert@SG-s01-01:0]# member 2_3`
4	Disable the global mode.	`set global-mode off`	This makes sure that the new snapshot image is created only on this SGM.
5	Create a new snapshot image.	`add snapshot <Snapshot_Name> desc "<Snapshot Description>"`	Example: `[Global] SG-s01-01 > add snapshot <Snapshot_Working_SGM> desc "Snapshot of a working SGM #3 on the Standby Chassis"`
6	Monitor the progress of the snapshot image creation.	`show snapshots`	Run this command repeatedly. The process can take 15 - 20 minutes.

<table>
<tr><th>Step</th><th>Procedure</th><th>Instructions</th><th>Notes</th></tr>
<tr><td>7</td><td>Insert a USB removable disk in the USB port of the SGM, and mount it to the <code>/mnt/usb</code> directory.</td><td>a. Find the device name for the USB removable disk in one of these ways:
■ In the <code>/var/log/messages</code> file:
<code>[Expert@SG-s01-01:0]# tail /var/log/messages</code>
Example:
<pre>:SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)
sdb: Write Protect is off
sdb: assuming drive cache: write through
SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)
sdb: Write Protect is off
sdb: assuming drive cache: write through
sdb: sdb1
sd 9:0:0:0: Attached scsi removable disk sdb
sd 9:0:0:0: Attached scsi generic sg1</pre>■ With the "<code>fdisk -l</code>" command:
<code>[Expert@SG-s01-01:0]# fdisk -l</code>
b. Create the <code>/mnt/usb</code> directory:
<code>[Expert@SG-s01-01:0]# mkdir -p /mnt/usb</code>
c. Mount the USB removable disk (for example: <code>/dev/sdb1</code>) to your <code>/mnt/usb</code> directory:
<code>[Expert@SG-s01-01:0]# mount /dev/sdb1 /mnt/usb</code></td><td></td></tr>
<tr><td>8</td><td>When the image creation is complete, export the snapshot image file to a TAR file on the local SGM.</td><td><code>set snapshot export <<i>Name of Snapshot Image File Without the .TAR Extension</i>> path /home/admin</code></td><td>Later, you copy this file to the USB device.</td></tr>
</table>

Step	Procedure	Instructions	Notes
9	Monitor the progress of the snapshot image creation.	`show snapshots`	Run this command repeatedly. The process can take 15 - 20 minutes.
10	Copy the snapshot file to the USB removable disk.	`[Expert@SG-s01-01:0]# cp -v /home/admin/<Name of Snapshot Image File Without the .TAR Extension>.tar /mnt/usb/`	
11	Check the snapshot image TAR file on the USB removable disk.	`[Expert@SG-s01-01:0]# ls -l /mnt/usb/`	
12	Unmount the USB removable disk from the `/usb/mnt` directory.	`[Expert@SG-s01-01:0]# umount /mnt/usb`	
13	Remove the USB removable disk from the SGM.		

Part 2- Required steps on the replacement SGM

Step	Procedure	Instructions	Notes
14	Insert the replacement SGM into a slot that is not part of any Security Group.		If all the slots are used, reconfigure the Security Group to remove one of the SGMs from it: `delete smo security-group <SGM ID>`
15	Connect to the command line on the replacement SGM.		
16	Disable the global mode.	`set global-mode off`	This makes sure that the new snapshot image applies only to this SGM.
17	Connect to the replacement SGM over a console connection.		

Step	Procedure	Instructions	Notes

18	Insert a USB removable disk in the USB port of the replacement SGM, and mount it to the `/mnt/usb` directory.	a. Find the device name for the USB removable disk in one of these ways:
		■ In the `/var/log/messages` file:
		`[Expert@SG-s01-01:0]# tail /var/log/messages`
		Example:
		`:SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)`
		`sdb: Write Protect is off`
		`sdb: assuming drive cache: write through`
		`SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)`
		`sdb: Write Protect is off`
		`sdb: assuming drive cache: write through`
		`sdb: sdb1`
		`sd 9:0:0:0: Attached scsi removable disk sdb`
		`sd 9:0:0:0: Attached scsi generic sg1`
		■ With the "`fdisk -l`" command:
		`[Expert@SG-s01-01:0]# fdisk -l`
		b. Create the `/mnt/usb` directory:
		`[Expert@SG-s01-01:0]# mkdir -p /mnt/usb`
		c. Mount the USB removable disk (for example: `/dev/sdb1`) to your `/mnt/usb` directory:
		`[Expert@SG-s01-01:0]# mount /dev/sdb1 /mnt/usb`	

19	Copy the snapshot file from the USB removable disk to the replacement SGM.	`[Expert@SG-s01-01:0]# cp -v /mnt/usb/<Name of Snapshot Image>.tar /home/admin/`	

Step	Procedure	Instructions	Notes
20	Import the snapshot image file.	`set snapshot import <Name of Snapshot Image File Without the .TAR Extension> path /home/admin/`	
21	Monitor the progress of the snapshot image import.	`show snapshots`	Run this command repeatedly. The process can take 15 - 20 minutes.
22	Unmount the USB removable disk from the `/mnt/usb` directory.	`[Expert@SG-s01-01:0]# umount /mnt/usb`	
23	Remove the USB removable disk from the replacement SGM.		
24	Revert the snapshot image.	`set snapshot revert <Snapshot_Name>`	Revert can take 15 - 20 minutes. During the revert, the SGM can reboot several times. Proceed to the next step after the revert is complete.
25	Connect to the command line on the chassis, over an SSH or console connection.		

Step	Procedure	Instructions	Notes
26	Log in to the Expert mode.	`expert`	
27	Update the Security Group to include the replacement SGM.	`add smo security-group <SGM ID>`	You can run this command: `add smo security_group {$NEW_SGM_ID}`
28	Confirm that the replacement SGM is in the state "`UP`" and enforces the latest policy.	`[Expert@SG-s01-01:0]# asg monitor`	
29	Confirm that all SGMs on the chassis have the same OS version.	`[Expert@SG-s01-01:0]# asg_version`	

Example

```
[Expert@SG-s01-01:0]# gclish

[Global] SG-s01-01 > set global-mode off

SG-s01-01 > add snapshot rma_62 desc rma
Taking snapshot. You can continue working normally.
You can use the command 'show snapshots' to monitor creation progress,

SG-s01-01 > show snapshots
Restore points:
---------------
armdilo62_2
Restore point now under creation:
riua_62 (19%)

Creation of an additional restore point will need 2.624G
Amount of space available for restore points is 1.41G

SG-s01-01 > show snapshots
Restore points:
----------------
rma_62
armdi 1062_2

Creation of an additional restore point will need 2.624G
Amount of space available for restore points is 41.53G

SG-s01-01 > set snapshot export rma_62 path /mnt/usb/
Exporting snapshot. You can continue working normally.
You can use the command 'show snapshots' to monitor exporting progress.

SG-s01-01 > set global-mode on

[Global] SG-s01-01 > exit

[Expert@SG-s01-01:0]# member 2_3
Moving to blade 2_3
This system is for authorized use only.
Last login: Wed Jun 20 08:43:28 2012 from SG-s02-03

[Expert@SG-s02-03:0]# cd /mnt/usb

[Expert@SG-s02-03:0]# ls
rzna_62.tar

[Expert@SG-s02-03:0]# umount /uint/usb
```

Installing a New SGM Using a CD/DVD Device

Step	Instructions
1	Burn the required image onto a CD/DVD. See the R82 Home Page: sk181127..
2	Install the new SGM into an unoccupied slot in the Standby Chassis.
3	If necessary, reconfigure the Security Group to include the new SGM.
4	Connect to the new SGM with a console connection.
5	Remove the SGM boot sector: `eraseboot`
6	Connect the CD/DVD device to the SGM.
7	Reboot the SGM: a. Pull it out b. Insert it
8	The installation starts. Follow the instructions in the console connection to the new SGM.

Replacing the CMM on Scalable Chassis

Install the replacement CMM that you received in the Return Merchandise Authorization (RMA).

These steps are for CMM installation on a Standby Chassis in a Dual Chassis environment.

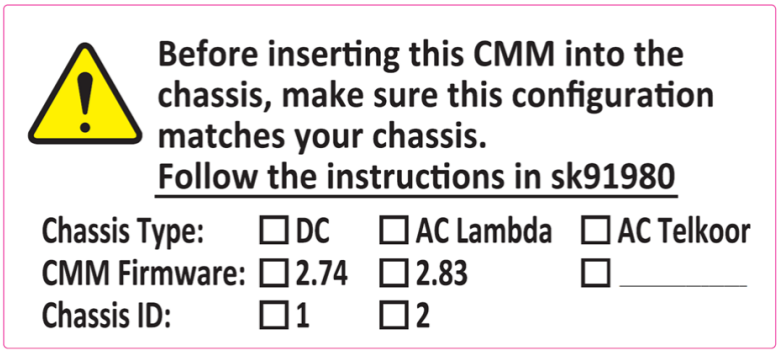
Prerequisites

1. Make sure you have a supported Standby Chassis type.

Standby Chassis Model	Supported Standby Chassis Type
44000	■ AC Telkoor - Three Telkoor power supplies ■ DC Standby Chassis

2. Get the label from the CMM box.

   Example:



3. Make sure that the Standby Chassis ID on the label on the outside of the CMM packaging box is the same as the label on the Standby Chassis.

   If the Chassis ID is different from the Chassis ID of the RMA CMM, change the RMA CMM Chassis ID. See *"Configuring the Chassis ID" on page 376*.

Replacing the CMM

Step	Instructions
1	Install the replacement CMM in the Standby Chassis.

Step	Instructions

2	Make sure that all CMMs in the environment have the same CMM firmware version:
	`asg_version -i`
	Example:
	`[Expert@SG-s01-01:0]# asg_version -i`
	`+----------+----------+----------+----------+`
	`| Hardware Versions |`
	`+----------+----------+----------+----------+`
	`| Component | Type | Configuration | Firmware |`
	`+----------+----------+----------+----------+`
	`| **Standby Chassis 1** |`
	`+----------+----------+----------+----------+`
	`| SSM1 | SSM440 | N/A | 5.5.x |`
	`| SSM2 | SSM440 | N/A | 5.5.x |`
	`| CMM(active) | N/A | N/A | **2.83** |`
	`| CMM(standby) | N/A | N/A | **2.83** |`
	`+----------+----------+----------+----------+`
	`+----------+----------+----------+----------+`
	`| Hardware Versions |`
	`+----------+----------+----------+----------+`
	`| Component | Type | Configuration | Firmware |`
	`+----------+----------+----------+----------+`
	`| **Standby Chassis 2** |`
	`+----------+----------+----------+----------+`
	`| SSM1 | SSM440 | N/A | 5.5.x |`
	`| SSM2 | SSM440 | N/A | 5.5.x |`
	`| CMM(active) | N/A | N/A | **2.83** |`
	`| CMM(standby) | N/A | N/A | **2.83** |`
	`+----------+----------+----------+----------+`
	`[Expert@SG-s01-01:0]#`

The output must be the same as the box label.

- If the CMM firmware versions are **not** the same, upgrade the CMM Firmware.

  See *"Upgrading Hardware Components on Scalable Chassis" on page 433*.

- If the Standby Chassis IDs are **not** the same, change the Standby Chassis ID on the RMA CMM.

  See *"Configuring the Chassis ID" on page 376*.

- If the Standby Chassis Types are **not** the same, follow the procedure *"Correcting an Incorrect Chassis Type" on the next page*.

Correcting an Incorrect Chassis Type

Step	Instructions
1	Connect to the command line on the Standby Chassis.
2	Log in to Gaia Clish.
3	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.
4	Change the state of the Standby Chassis to "Down": See *"set cluster sites-admin-state" on page 937*. `set cluster sites-admin-state id <ID of Standby Chassis> down`
5	Remove all CMMs from the Standby Chassis.
6	Insert only the replacement CMM in the Standby Chassis.
7	Open a console connection to the CMM: a. Connect one end of a serial cable to the serial port on the CMM front panel. b. Connect the other end of the serial cable to a computer. c. Open a console window in your terminal emulation program (for example, PuTTY, SecureCRT). Use the default serial connection parameters: 9600, 8, N, 1
8	Start the installation: `install.sh`
9	Insert the second CMM.
10	On the 41000 and 44000 chassis models: When the option to upgrade `EEprom` appears, select option `1`. `---------- | EEprom upgrading | 1: Press 1 for EEProm upgrading. | 2. Press 2 to skip. | ----------` **Note** - On the 60000 chassis models, there is no need to upgrade the EEprom.
11	Change the state of the Standby state to "Up": `set cluster sites-admin-state id <ID of Standby Chassis> up`

Troubleshooting on Scalable Chassis

This section provides troubleshooting commands on Scalable Chassis.

Log Files on Scalable Chassis

Below are the log files on the Chassis:

Feature	Debug File
Alerts	`/var/log/send_alert.*`
Command auditing	`/var/log/asgaudit.log*`
CPD	`$CPDIR/log/cpd.elg`
Distribution	`/var/log/dist_mode.log*`
Dynamic Routing	`/var/log/routed.log`
Expert mode shell auditing	`/var/log/command_logger.log*`
FWD	`$FWDIR/log/fwd.elg`
FWK	`$FWDIR/log/fwk.elg.*`
Gaia Clish auditing	`/var/log/auditlog*`
Gaia First Time Configuration Wizard	`/var/log/ftw_install.log`
General	`/var/log/messages*`
SMO Image Cloning	`/var/log/image_clone.log.dbg*`
Installation	`/var/log/start_mbs.log`
Installation - OS	`/var/log/anaconda.log`
Log Servers	`/var/log/log_servers*`
Policy	`$FWDIR/log/cpha_policy.log.*`
Reboot logs	`/var/log/reboot.log`
SGM Configuration Pull Configuration	`$FWDIR/log/blade_config.*`
VPND	`$FWDIR/log/vpnd.elg*`

Common Procedures for Scalable Platforms

This chapter describes the procedures that apply all HyperScale products.

The unique procedures are described here:

- **ElasticXL Cluster** - see *"Working with ElasticXL Cluster" on page 30*.
- **Quantum Maestro** - see *"Working with Quantum Maestro" on page 48*.
- **Quantum Scalable Chassis** - see *"Working with Quantum Scalable Chassis" on page 270*.

Rolling Back a Failed Upgrade of a Security Group from R82 - Zero Downtime (MVC)

This section describes the steps to roll back a failed upgrade of a Security Group from R82 with Zero Downtime - as a Multi-Version Cluster (MVC).

For upgrade procedures, see:

- *"Upgrading Maestro Environment to R82" on page 52*
- *"Upgrading Scalable Chassis to R82 - Zero Downtime (MVC)" on page 272*

This section describes the steps for rolling back a failed upgrade of a Security Group to R82.

This procedure supports only these downgrade paths for Security Groups:

- from R82 to R81.20
- from R82 to R81.10
- from R82 to R81

Warnings:

- Multi-Version Cluster (Zero Downtime) downgrade from R82 to R81.10 / 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.

Rolling Back If Only Some of the Security Group Members Were Upgraded - Zero Downtime

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 the Expert mode (`/bin/bash`), then go to the Gaia gClish: `gclish`

Step	Instructions

3	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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.
	a. Examine the state of the SMO Image Cloning feature:
	`show cluster configuration image auto-clone state`
	See *"show cluster configuration image" on page 964*.
	b. Disable the SMO Image Cloning feature, if it is enabled:
	`set cluster configuration image auto-clone state off`
	See *"set cluster configuration image" on page 930*.
	c. Examine the state of the SMO Image Cloning feature:
	`show cluster configuration image auto-clone state`

4	Go to the Expert mode:
	■ If your default shell is the Expert mode (`/bin/bash`):
	`exit`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`):
	`expert`

5	Go to the context of one of the Security Group Members that were upgraded to R82:
	`member <Member ID>`
	See *"member" on page 909*.
	Example:
	`member 1_1`

6	On **each** Security Group Member that was upgraded to R82, restore the Gaia snapshot that was automatically created before the upgrade.

Step	Instructions

	In Dual Site, follow these steps to restore a Gaia snapshot:
	Procedure
	a. Do these steps on **each** upgraded Security Group Member on the Standby Site:
	i. Go to the context of the upgraded Security Group Member:
	`member <ID of Security Group Member>`
	Example:
	`member 2_5`
	ii. Go to Gaia Clish (do **not** use the Gaia gClish):
	`clish`
	iii. Restore the Gaia snapshot that was saved automatically before the upgrade.
	`set snapshot revert AutoSnapShot_<Original-Version>_<Take>`
	Example:
	`set snapshot revert AutoSnapShot_AutoSnapShot_R8120_47`
	iv. Wait for the Security Group Member to complete the reboot.
	b. After you revert **each** upgraded Security Group Member on the Standby Site, examine the state of all Security Group Members (write down the ID of the Standby Site):
	`asg stat`
	See *"asg stat" on page 829*.
	Note - By design, the state of the reverted Security Group Members will be "`DOWN`".
	c. Change the state of all Security Group Members to "`UP`" on the Standby Site.
	`g_clusterXL_admin -b {chassis1 | chassis2} up`
	See *"g_clusterXL_admin" on page 896*.
	Where:
	▪ `chassis1` - Applies to all Security Group Members on Site 1
	▪ `chassis2` - Applies to all Security Group Members on Site 2
	d. Make sure all Security Group Members are in the state "`ACTIVE`":
	`asg stat`
	e. Manually fail over from the Active Site to the Standby Site:

Step	Instructions
	``` g_clusterXL_admin -b {chassis1 | chassis2} down ``` Where: ■ `chassis1` - Applies to all Security Group Members on Site 1 ■ `chassis2` - Applies to all Security Group Members on Site 2 f. Examine the state of all Security Group Members: ``` asg stat ``` g. Repeat Steps **6, a-d** for Dual Site on each upgraded Security Group Member on the former Active Site. At the end of this procedure all Security Group Members must be in the state "`ACTIVE`".

Step	Instructions

	In Single Site, follow these steps to restore a Gaia snapshot:
	Procedure
	a. Do these steps on **each** upgraded Security Group Member:
	i. Go to the context of the upgraded Security Group Member:
	`member <ID of Security Group Member>`
	Example:
	`member 1_5`
	ii. Go to Gaia Clish (do **not** use the Gaia gClish):
	`clish`
	iii. Restore the Gaia snapshot that was saved automatically before the upgrade.
	`set snapshot revert AutoSnapShot_<Original-Version>_<Take>`
	Example:
	`set snapshot revert AutoSnapShot_AutoSnapShot_R8120_47`
	iv. Wait for the Security Group Member to complete the reboot.
	b. After you revert **each** upgraded Security Group Member, examine the state of all Security Group Members:
	`asg stat`
	See *"asg stat" on page 829*.
	Note - By design, the state of the reverted Security Group Members will be "`DOWN`".
	c. Change the state of all reverted Security Group Members to "`UP`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	`g_clusterXL_admin -b <ID of first selected SGM> up`
	`g_clusterXL_admin -b <ID of second selected SGM> up`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_4 up`
	`g_clusterXL_admin -b 1_6 up`
	`g_clusterXL_admin -b 1_8 up`
	See *"g_clusterXL_admin" on page 896*.
	d. Make sure all Security Group Members are in the state "`ACTIVE`":

Step	Instructions
	`asg stat`

11	Make sure the downgrade was successful.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

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.
- 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	If your default shell is the Expert mode (`/bin/bash`), then go to the Gaia gClish: `gclish`

Step	Instructions

3	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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.
	a. Examine the state of the SMO Image Cloning feature:
	`show cluster configuration image auto-clone state`
	See *"show cluster configuration image" on page 964*.
	b. Disable the SMO Image Cloning feature, if it is enabled:
	`set cluster configuration image auto-clone state off`
	See *"set cluster configuration image" on page 930*.
	c. Examine the state of the SMO Image Cloning feature:
	`show cluster configuration image auto-clone state`

4	Go to the Expert mode:
	■ If your default shell is the Expert mode (`/bin/bash`):
	`exit`
	■ If your default shell is Gaia gClish (`/etc/gcli.sh`):
	`expert`

5	Go to the context of one of the Security Group Members that were upgraded to R82:
	`member <Member ID>`
	See *"member" on page 909*.
	Example:
	`member 1_1`

6	On **each** Security Group Member that was upgraded to R82, restore the Gaia snapshot that was automatically created before the upgrade.

Step	Instructions

	In Dual Site, follow these steps to restore a Gaia snapshot:
	Procedure
	a. Do these steps on **each** upgraded Security Group Member on the Standby Site:
	i. Go to the context of the upgraded Security Group Member:
	`member <ID of Security Group Member>`
	Example:
	`member 2_5`
	ii. Go to Gaia Clish (do **not** use the Gaia gClish):
	`clish`
	iii. Restore the Gaia snapshot that was saved automatically before the upgrade.
	`set snapshot revert AutoSnapShot_<Original-Version>_<Take>`
	Example:
	`set snapshot revert AutoSnapShot_ AutoSnapShot_R8120_47`
	iv. Wait for the Security Group Member to complete the reboot.
	b. After you revert **each** upgraded Security Group Member on the Standby Site, examine the state of all Security Group Members (write down the ID of the Standby Site):
	`asg stat`
	See *"asg stat" on page 829*.
	Note - By design, the state of the reverted Security Group Members will be "`DOWN`".
	c. Change the state of all Security Group Members to "`UP`" on the Standby Site.
	`g_clusterXL_admin -b {chassis1 | chassis2} up`
	See *"g_clusterXL_admin" on page 896*.
	Where:
	■ `chassis1` - Applies to all Security Group Members on Site 1
	■ `chassis2` - Applies to all Security Group Members on Site 2
	d. Make sure all Security Group Members are in the state "`ACTIVE`":
	`asg stat`
	e. Manually fail over from the Active Site to the Standby Site:

Step	Instructions
	``` g_clusterXL_admin -b {chassis1 | chassis2} down ``` Where: ■ `chassis1` - Applies to all Security Group Members on Site 1 ■ `chassis2` - Applies to all Security Group Members on Site 2 f. Examine the state of all Security Group Members: ``` asg stat ``` g. Repeat Steps **6, a-d** for Dual Site on each upgraded Security Group Member on the former Active Site. At the end of this procedure all Security Group Members must be in the state "`ACTIVE`".

Step	Instructions

	In Single Site, follow these steps to restore a Gaia snapshot:
	Procedure
	Divide all Security Group Members into two logical groups - Logical Group "A" (for example 1_1-1_4) and Logical Group "B" (for example, 1_5-1_8).
	a. Do these steps on **each** upgraded Security Group Member in the Logical Group "A":
	i. Go to the context of the upgraded Security Group Member:
	`member <ID of Security Group Member>`
	Example:
	`member 1_1`
	ii. Go to Gaia Clish (do **not** use the Gaia gClish):
	`clish`
	iii. Restore the Gaia snapshot that was saved automatically before the upgrade.
	`set snapshot revert AutoSnapShot_<Original-Version>_<Take>`
	Example:
	`set snapshot revert AutoSnapShot_ AutoSnapShot_R8120_47`
	iv. Wait for the Security Group Member to complete the reboot.
	b. After you revert **each** upgraded Security Group Member in the Logical Group "A", examine the state of all Security Group Members:
	`asg stat`
	Note - By design, the state of the reverted Security Group Members will be "`DOWN`".
	See *"asg stat" on page 829*.
	c. Change the state of all reverted Security Group Members in the Logical Group "A" to "`UP`":
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	`g_clusterXL_admin -b <ID of first selected SGM in Group "A"> up`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "A"> up`
	`and so on`

Step	Instructions

	See *"g_clusterXL_admin" on page 896*.
	Example:
	`g_clusterXL_admin -b 1_1 up`
	`g_clusterXL_admin -b 1_2 up`
	`g_clusterXL_admin -b 1_3 up`
	`g_clusterXL_admin -b 1_4 up`
	d. Examine the state of all Security Group Members:
	`asg stat`
	e. Manually fail over from the Security Group Members in the Logical Group "B" (not reverted yet) to the Security Group Members in the Logical Group "A" (already reverted):
	Best Practice - To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.
	`g_clusterXL_admin -b <ID of first selected SGM in Group "B"> down`
	`g_clusterXL_admin -b <ID of second selected SGM in Group "B"> down`
	`and so on`
	Example:
	`g_clusterXL_admin -b 1_5 down`
	`g_clusterXL_admin -b 1_6 down`
	`g_clusterXL_admin -b 1_7 down`
	`g_clusterXL_admin -b 1_8 down`
	f. Examine the state of all Security Group Members:
	`asg stat`
	g. Repeat Steps **6, a-d** for Single Site on each upgraded Security Group Member in the Logical Group "B".
	At the end of this procedure all Security Group Members must be in the state "`ACTIVE`".

Step	Instructions

7	Make sure the downgrade was successful.
	Use one of these tools:
	■ The "`insights`" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Installing and Uninstalling a Hotfix on Security Group Members

This section describes the Full Connectivity installation and uninstall of an Offline CPUSE package.

Important Notes

This procedure is supported only on these:

- Maestro Security Group
- ElasticXL Cluster

Notes:

- The procedure term "Site" applies to Maestro Security Group and to ElasticXL Cluster.
- The procedure term "Security Group" applies to Maestro Security Group and to ElasticXL Cluster.
- The procedure term "Security Group Member" applies to a Maestro Security Group Member and to an ElasticXL Cluster Member.
- The procedure term "Security Group Members" applies to Maestro Security Group Members and to ElasticXL Cluster Members.
- ElasticXL Cluster supports a maximum of:
  - 3 ElasticXL Cluster Members on each ElasticXL Site.
  - 6 ElasticXL Cluster Members in total.
- CPUSE examples below are provided for a Maestro Security Group.

Notes:

- For Scalable Chassis, see *"Installing and Uninstalling a Hotfix on SGMs on Scalable Chassis" on page 317*.
- For information about the CLI commands for Scalable Platforms, see *"Working with Command Line" on page 686*.
- For information about the CLI commands for CPUSE, see sk92449.

Installing a Hotfix Package on Security Group Members

Important:

- This procedure keeps the current connections in a Security Group.
- In Maestro: This procedure applies to Security Groups in the Security Gateway, VSNext, and Traditional VSX modes.

  In the VSNext mode, you must run all the commands in the context of the Virtual Gateway 0.

  In the Traditional VSX mode, you must run all the commands in the context of VS0.
- In ElasticXL: This procedure applies to Security Groups in the Security Gateway and in the VSNext modes.

  In the VSNext mode, you must run all the commands in the context of the Virtual Gateway 0.
- **Do not install the hotfix on all the Security Group Members in a Security Group at the same time.**
- In this procedure, you divide all Security Group Members in a 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.

  1. You fail over from the Logical Group "A" to the Logical Group "B".
  2. You install the hotfix on the Logical Group "A" while the Logical Group "B" continues to handle traffic.
  3. You fail over from the Logical Group "B" to the Logical Group "A".
  4. You install the hotfix on the Logical Group "B" while the Logical Group "A"

continues to handle traffic.

Examples

Environment	Description
Maestro Single Site	• 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.
Maestro Single Site	• 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 from 1_4 to 1_5.
Maestro Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.
ElasticXL Single Site	• There are 3 ElasticXL Cluster Members in the ElasticXL Cluster. • The Logical Group "A" contains ElasticXL Cluster Members from 1_1 to 1_2. • The Logical Group "B" contains the ElasticXL Cluster Member 1_3.
ElasticXL Dual Site	• There are 6 ElasticXL Cluster Members in the ElasticXL Cluster (3 on each Site). • The Logical Group "A" contains ElasticXL Cluster Members on Site 1 from 1_1 to 1_3. • The Logical Group "B" contains ElasticXL Cluster Members on Site 2 from 2_1 to 2_3.

Installation Procedure

Hotfix Installation 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 `/var/log/`).
C	Connect to the command line on the Security Group.
D	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`

E	Import the CPUSE Offline package from the hard disk:
	`installer import local /<Full Path>/<Name of the CPUSE Offline Package>`
	Example:
	`[Global] SG-s01-01 > installer import local /var/log/Check_Point_R82_Hotfix_Bundle_FULL.tgz`

F	Show the imported CPUSE packages: `show installer packages imported`

Step	Instructions

G	Make sure the imported CPUSE package can be installed on this Security Group:
	`installer verify [Press the Tab key]`
	`installer verify <Number of CPUSE Package> member_ids all`
	Example:
	`[Global] SG-s01-01 > 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] SG-s01-01 >`

Hotfix Installation 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show cluster configuration image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set cluster configuration image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show cluster configuration image auto-clone state`

Hotfix Installation Step 3 - Install the Hotfix on the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group **"A" through the console**. ■ Connect to one of the Security Group Members in the Logical Group **"B" over SSH**.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`

C	Set the Security Group Members in the Logical Group "A" to the state "`DOWN`":
	`set cluster members-admin-state ids <SGM IDs in Group "A"> down`
	Example:
	`set cluster members-admin-state ids 1_1-1_4 down`

D	Connect to one of the Security Group Members in the Logical Group "A":
	`member <Member ID>`
	Example:
	`member 1_1`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is the Expert mode, then run:
	`gclish`
	■ If your default shell is Gaia Clish (`/etc/cli.sh`), then run:
	`exit`

Step	Instructions

F	Install the CPUSE hotfix package on the Security Group Members in the Logical Group "A":
	`installer install [Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] SG-s01-01 > 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) y`
	`[Global] SG-s01-01 >`

G	Monitor the system until the Security Group Members in the Logical Group "A" are in the state "UP" and enforce the Security Policy again: `show cluster info overview live`

Hotfix Installation Step 4 - Install the Hotfix on the Security Group Members in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**B**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**A**" **over SSH**.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`

C	Set the Security Group Members in the Logical Group "B" to the state "`DOWN`":
	`set cluster members-admin-state ids <SGM IDs in Group "B"> down`
	Example:
	`set cluster members-admin-state ids 1_5-1_8 down`

D	Connect to one of the Security Group Members in the Logical Group "B":
	`member <Member ID>`
	Example:
	`member 1_5`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is the Expert mode, then run:
	`gclish`
	■ If your default shell is Gaia Clish (`/etc/cli.sh`), then run:
	`exit`

Step	Instructions

F	Install the CPUSE hotfix package on the Security Group Members in the Logical Group "B":
	`installer install [Press the Tab key]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] SG-s01-01 > 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) y`
	`[Global] SG-s01-01 >`

G	Monitor the system until the Security Group Members in the Logical Group "B" are in the state "UP" and enforce the security policy again: `show cluster info overview live`

Hotfix Installation 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	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`

C	Use one of these tools:
	■ The "insights" tool (see *"insights" on page 903*):
	`insights`
	■ The HCP tool (see *"hcp" on page 899*):
	`hcp --help`

Uninstalling a Hotfix Package on Security Group Members

Important:

- This procedure keeps the current connections in a Security Group.
- In Maestro: This procedure applies to Security Groups in the Security Gateway, VSNext, and Traditional VSX modes.

  In the VSNext mode, you must run all the commands in the context of the Virtual Gateway 0.

  In the Traditional VSX mode, you must run all the commands in the context of VS0.
- In ElasticXL: This procedure applies to Security Groups in the Security Gateway and in the VSNext modes.

  In the VSNext mode, you must run all the commands in the context of the Virtual Gateway 0.
- **Do not uninstall the hotfix from all the Security Group Members in a Security Group at the same time.**
- In this procedure, you divide all Security Group Members in a Security Group into two or more logical groups.

  In the procedure below, we use **two** logical groups denoted below as "**A**" and "**B**".

  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.

  Each logical group should contain the same number of Security Group Members - as close as possible.

  1. You fail over from the Logical Group "A" to the Logical Group "B".
  2. You uninstall the hotfix from the Logical Group "A" while the Logical Group "B" continues to handle traffic.
  3. You fail over from the Logical Group "B" to the Logical Group "A".
  4. You uninstall the hotfix from the Logical Group "B" while the Logical Group "A"

continues to handle traffic.

Examples

Environment	Description
Maestro Single Site	• 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.
Maestro Single Site	• 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 from 1_4 to 1_5.
Maestro Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.
ElasticXL Single Site	• There are 3 ElasticXL Cluster Members in the ElasticXL Cluster. • The Logical Group "A" contains ElasticXL Cluster Members from 1_1 to 1_2. • The Logical Group "B" contains the ElasticXL Cluster Member 1_3.
ElasticXL Dual Site	• There are 6 ElasticXL Cluster Members in the ElasticXL Cluster (3 on each Site). • The Logical Group "A" contains ElasticXL Cluster Members on Site 1 from 1_1 to 1_3. • The Logical Group "B" contains ElasticXL Cluster Members on Site 2 from 2_1 to 2_3.

Uninstall Procedure

Hotfix Uninstall 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. Note - Enable the SMO Image Cloning feature only before you need to add a new Security Group Member and disable it immediately after it joins the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show cluster configuration image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set cluster configuration image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature again: `show cluster configuration image auto-clone state`

Hotfix Uninstall Step 2 - Uninstall the Hotfix from the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**A**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**B**" **over SSH**.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`

C	Set Security Group Members in the Logical Group "A" to the state "DOWN":
	`set cluster members-admin-state ids <SGM IDs in Group "A"> down`
	Example:
	`set cluster members-admin-state ids 1_1-1_4 down`

D	Connect to one of the ElasticXL Cluster Members in the Logical Group "A":
	`member <ID of Site>_<Member ID>`
	Example:
	`member 1_1`

E	Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "A":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] SG-s01-01 > 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] SG-s01-01 >`

Step	Instructions
F	Monitor the system until the Security Group Members in the Logical Group "A" are in the state "UP" and enforce the Security Policy again: `show cluster info overview live`

Hotfix Uninstall Step 3 - Uninstall the Hotfix from the Security Group Members in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**B**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**A**" **over SSH**.
B	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`

C	Set Security Group Members in the Logical Group "B" to the state "DOWN":
	`set cluster members-admin-state ids <SGM IDs in Group "B"> down`
	Example:
	`set cluster members-admin-state ids 1_5-1_8 down`

D	Connect to one of the ElasticXL Cluster Members in the Logical Group "B":
	`member <ID of Site>_<Member ID>`
	Example:
	`member 1_5`

E	Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "B":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] SG-s01-05 > 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] SG-s01-05 >`

Step	Instructions
F	Monitor the system until the Security Group Members in the Logical Group "B" are in the state "UP" and enforce the Security Policy again: `show cluster info overview live`

Hotfix Uninstall 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	If your default shell is the Expert mode, then go to Gaia gClish: `gclish`
C	Get the list of the installed packages: `show installer packages installed`

Managing Security Groups

This section provides basic information about managing Security Groups.

Single Management Object and Policies

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 *"asg stat" on page 829*).

Example output in a Maestro Single Site configuration

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

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example output in a Maestro 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@SG-s01-01:0]# 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@SG-s01-01:0]#
[Expert@SG-s01-01:0]# member 2_4
Moving to member 2_4
... ...
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

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

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

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: `asg policy unload`

Working with Policies in CLI

See *"asg_policy" on page 797*.

Policy Management on Security Group Members

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: `asg_blade_config pull_config`

2	Do **one** of these:
	■ Reboot the **target** Security Group Member:
	`reboot -b <Security Group Member ID>`
	■ Start the Check Point services and remove the ClusterXL Critical Device "`admin_down`":
	`cpstart`
	`clusterXL_admin up`

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
`global_context`	`$FWDIR/boot/modules/fwkern.conf`	`/bin/false`

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@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Global Commands on Security Groups

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.

  See the *R82 Gaia Administration Guide*.

Gaia Global 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:

Global Command in Gaia gClish	Global Command in the Expert mode
`arp`	`g_arp` `g_allc 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
<Gaia gClish Command>	Standard command in Gaia gClish as appears in the table above.
<Global Expert mode Command>	Global command in the Expert mode as appears in the table above.
`-b` *<SGM IDs>*	Applies to Security Group Members as specified by the *<SGM IDs>*. *<SGM IDs>* can be: ■ No *<SGM IDs>* specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`) **Note** - You can only select Security Group Members from one Site with this option.

Parameter	Description
<Command Options>	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@SG-s01-01:0]# 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@SG-s01-01:0]#
```

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 gClish:

```
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 (`~/.toprc`) on the local Security Group Member.
`-f`	Exports the output to a file. Default: `/vat/log/gtop.<Time>`
`-o <Output File>`	Specifies the path and name of the output file. Must use with the "`-f`" parameter.
`-n <Number of Iterations>`	The command saves the output the specified number of times. Default: 1 Must use with the "`-f`" parameter.
`-s <Output File>`	Shows the content of the output file `<Output File>`, in which the command saved its output earlier.
`<Command Options>`	Parameters of the standard `top` command. For more information, see the `top` 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: `top`
4	Set the desired view (press **h** to see the built-in help).

Step	Instructions
5	Press **Shift+W** to save the '`top`' configuration.
6	Run: `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@SG-s01-01:0]# gclish
[Global] SG-s01-01 > 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] SG-s01-01 >
```

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 Gaia gClish	`fw` `fw6`
Expert mode	`g_fw` `g_fw6`

Examples

Example 1

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01 >
```

Example 2

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01 >
```

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] SG-s01-01 > fw dbgfile collect -f /var/log/debug.txt -buf 8200 -m fw + conn -m kiss + pmdump
```

Example - Show the collected debug information

```
[Global] SG-s01-01 > fw dbgfile view /var/log/debug.txt
```

Important - For complete debug procedure, see the *R82 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	`fwaccel help`	`fwaccel6 help`
Expert mode	`g_fwaccel help`	`g_fwaccel6 help`

Parameters and Options

For more information, see the *R82 Performance Tuning Administration Guide* > Chapter *SecureXL* > Section *SecureXL Commands and Debug* - Subsection *'fwaccel' and 'fwaccel6'*.

Backing Up and Restoring Gaia Configuration

For more information, see the *R82 Gaia Administration Guide*:

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

Working with the Distribution Mode

Background

- In ElasticXL Cluster:

  The ElasticXL Cluster uses the Distribution Mode to assign incoming traffic to Security Group Members in the ElasticXL Cluster.

  By default, the ElasticXL Cluster automatically configures the Distribution Mode.

- In Maestro:

  The Maestro Orchestrators use the Distribution Mode to assign incoming traffic to Security Group Members in each Security Group.

  By default, the Orchestrators automatically configure the Distribution Mode.

- On Scalable Chassis:

  The Security Switch Modules (SSMs) use the Distribution Mode to assign incoming traffic to Security Group Members in each Security Group.

  By default, the SSMs automatically configure the Distribution Mode.

Supported Distribution Modes

Mode	Instructions
User (Internal)	Packets are assigned to a Security Group Member based only on the packet's Destination IP address. If Layer 4 distribution is enabled, the ElasticXL Cluster / Maestro Orchestrator / Scalable Chassis SSM assigns packets to a Security Group Member based on the packet's Source Port and the Destination IP address. On Scalable Chassis, this mode applies to one SSM. **Note** - Scalable Platforms do not support Hide NAT when the Distribution Mode "User (Internal)" is configured on one of more outbound interfaces (Known Limitation SPC-1682).
Network (External)	Packets are assigned to a Security Group Member based only on the packet's Source IP address. If Layer 4 distribution is enabled, the ElasticXL Cluster / Maestro Orchestrator / Scalable Chassis SSM assigns packets to a Security Group Member based on the packet's Source IP address and Destination Port. On Scalable Chassis, this mode applies to one SSM. **Note** - Scalable Platforms do not support Hide NAT when the Distribution Mode "Network (External)" is configured on one or more inbound interfaces (Known Limitation SPC-1682).

Mode	Instructions
General	The ElasticXL Cluster / Maestro Orchestrators / Scalable Chassis SSMs assign packets to a Security Group Member based only on the packet's Source IP address and the Destination IP address. If Layer 4 distribution is enabled, the ElasticXL Cluster / Maestro Orchestrators / SSMs assign packets to a Security Group Member based on the packet's Source IP address, Source Port, Destination IP address, and Destination Port. On Scalable Chassis, this mode applies to all SSMs in the Scalable Chassis.
Auto-Topology (Per-Port) (default)	Each port for a Security Group Member is configured separately in the User Mode or Network Mode. On Scalable Chassis, this mode applies to the SSM data interface.

Notes:

- The default mode is **Auto-Topology** (**Per-Port**) and the Layer 4 distribution is disabled.
- 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.

Related Commands

- *"asg_dxl" on page 738*

Automatic Distribution Configuration (Auto-Topology)

Platform	Default Distribution Mode
ElasticXL Cluster	By default, Security Groups work in the **Auto-Topology** (**Per Port**) Mode with Layer 4 distribution disabled.
Maestro	By default, Security Groups work in the **Auto-Topology** (**Per Port**) Mode with Layer 4 distribution disabled.
Scalable Chassis	By default, Security Groups work in the **Auto-Topology** (**Per Port**) Mode with Layer 4 distribution disabled.

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

The examples below show how the Distribution Mode can be configured automatically for each interface.

Example 1 for Scalable Chassis - All ports on each SSM are Internal or External

The Distribution Mode for the two SSMs is automatically configured as the **User** (**Internal**) Mode or the **Network** (**External**)Mode.

Physical Interface	Topology	SSM	Distribution Mode
`eth1-01`	Internal	1	**User** (**Internal**)
`eth1-02`	Internal		
`eth2-01`	External	2	**Network** (**External**)
`eth2-02`	External		

Example 2 for Scalable Chassis - On at least one of the SSMs, some ports are Internal and others are External

The Distribution Mode for the SSMs is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	SSM	Port	Distribution Mode
eth1-01	Internal	1	1	**User** (**Internal**)
eth1-02	External	1	2	**Network** (**External**)
eth2-01	External	2	1	**Network** (**External**)
eth2-02	External	2	2	**Network** (**External**)

Example 3 for Scalable Chassis - Physical and VLAN Interfaces

Three VLANs are defined on one SSM port.

On at least one of the SSMs, some VLANs are Internal and others are External.

Therefore, the SSM Distribution Mode is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	SSM	Port	VLAN ID	Distribution Mode
eth1-01	External	1	1	NA	**Network** (**External**)
eth1-01.100	Internal	1	1	100	**User** (**Internal**)
eth1-01.200	External	1	1	200	**Network** (**External**)
eth1-01.300	Internal	1	1	300	**User** (**Internal**)

Example 4 for Scalable Chassis - Traditional VSX Virtual Systems

A Virtual Switch does not have topology.

Therefore, the Distribution Mode is calculated based on the topologies of the `wrp` interfaces that belong to Virtual Systems, as shown.

In this example, the Distribution Mode is calculated as **Network** (**External**).

Interface	Topology	Distribution Mode
`eth1-01`	External	Not Available
`wrp64`	Internal	**Network** (**External**)
`wrp128`	Internal	**Network** (**External**)
`wrp192`	Internal	**User** (**Internal**)

Example 5 for Scalable Chassis - Bond Interfaces

In this example, the interfaces on each Bond are configured with the same Distribution Mode.

The two Bond interfaces are configured with one port for SSM #1 and one port for SSM #2.

On the two SSMs, one port is Internal and the other is External.

The SSM Distribution Mode is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	Slaves	SSM	Port	VLAN ID
`bond1`	Internal	`eth1-01`	1	1	**User** (**Internal**)
`eth2-01`	2	1	User		
`bond2`	External	`eth1-02`	1	2	**Network** (**External**)
`eth2-02`	2	2	Network		

Example 6 for Scalable Chassis - VLAN Over Bond Interfaces

The automatic Distribution Mode configuration is based on the VLAN topology.

In this example, the interfaces on each VLAN are configured with the same Distribution Mode.

The two Bond interfaces are configured on port 1 for each SSM.

The SSM Distribution Mode is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	Slaves	SSM	Port	VLAN ID	Distribution Mode
bond1.100	Internal	eth1-01	1	1	100	**User** (**Internal**)
eth2-01	2	1	100	User		
bond1.200	External	eth1-01	1	1	200	**Network** (**External**)
eth2-01	2	1	200	Network		

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 configured manually (the **Manual-General** Mode), the Distribution Mode of ElasticXL Cluster / each Maestro Orchestrator / Scalable Chassis SSM is **General**.

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

Best Practice - Do **not** manually change the Distribution Mode of a Legacy 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.

Important - If the Security Group runs in the Legacy 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	Description
`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	Description

`ip-mask <Mask>`	Must be the same as the distribution matrix size.
	Must be specified in the Hex format.
	Follow these steps:
	1. Examine the distribution matrix size:
	`show distribution verification verbose`
	Examine the `Matrix Size` line.
	Example:
	`... Matrix Size 512 ...`
	2. Exit from the Gaia gClish to the Expert mode.
	3. Convert the matrix size from the decimal to the hexadecimal format:
	`printf '%x\n' <Matrix Size>`
	Example:
	`[Expert@SG-s01-01:0]# printf '%x\n' 512 200 [Expert@SG-s01-01:0]#`
	4. Go to the Gaia gClish:
	`gclish`
	5. Configure the distribution mode with the required mask:
	`set distribution ... ip-mask <Matrix Size in HEX>`
	Example:
	`set distribution ... ip-mask 200`

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 Traditional 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 **User** (**Internal**) Distribution Mode - based on the Destination IP address.
`network`	Manually assign the **Network** (**External**) Distribution Mode - based on the Source IP address.
`policy`	Use **Auto-Topology** to automatically assign the Distribution Mode according to the policy.

Examples

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

```
[Global] SG-s01-01 > 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] SG-s01-01 > 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] SG-s01-01 > 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 from a Maestro Security Group

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> show distribution status
distribution:
  l4_mode: 'on'
  mode: general
matrix:
  actual_size: '512'
ports:
  eth1-05: policy-internal
  eth1-06: policy-internal
[Global] SG-s01-01>
```

Example 2 - Regular output from a Scalable Chassis

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > show distribution status
Topic:                                  Configuration:
distribution mode                       per-port
policy mode                             on
ssm 1 mode                              per-port
ssm 2 mode                              per-port
ipv6 mode                               off
L4 mode                                 off
40g mode                                off
matrix size                             1024
[Global] SG-s01-01 >
```

Example 3 - Verbose output from a Maestro Security Group

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

Example 4 - Verbose output from a Scalable Chassis

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > show distribution status verbose
Topic:                                  Configuration:
distribution mode                       per-port
policy mode                             on
ssm 1 mode                              per-port
ssm 2 mode                              per-port
ipv6 mode                               off
L4 mode                                 off
40g mode                                off
matrix size                             1024
interface bond1.300 mode                policy-internal
interface bond2.33 mode                 policy-external
interface bond1 slaves                  eth1-01,eth2-01
interface bond2 slaves                  eth1-02,eth2-02
mask ipv4 general destination           0000001f
mask ipv4 general source                0000001f
mask ipv4 l4 ip                         000003ff
mask ipv4 l4 port                       00000000
mask ipv4 user-network destination      000003ff
mask ipv4 user-network source           000003ff
mask ipv6 general destination           0000000000000000000000000000001f
mask ipv6 general source                0000000000000000000000000000001f
mask ipv6 user-network destination      000000000000000000000000000003ff
mask ipv6 user-network source           000000000000000000000000000003ff

Total GW topology interfaces            2
Total GW topology VLANs                 2
Total SSM 1 interfaces                  17
Total SSM 2 interfaces                  17

Per interface distribution legend:
         Internal (User)        - Destination IP based
         External (Network)     - Source IP based
         General                - Source and Destination IP based

[Global] SG-s01-01 >
```

Explanation about the output for a Maestro Security Group

Field	Instructions
`L4 Mode`	Shows the Layer 4 distribution status: ■ `on` - enabled ■ `off` - disabled
`Mode`	Shows the currently configured Distribution Mode: ■ `per-port` - Auto-Topology ■ `user` - User (Internal) ■ `network` - Network (External) ■ `general` - General
`Matrix Size`	Shows the size of the Distribution Mode matrix.
`Ports`	Shows the Distribution Mode assignment for each interface.

Explanation about the output for a Scalable Chassis

Field	Instructions
`distribution mode`	Shows the currently configured Distribution Mode: ■ `per-port` - Auto-Topology ■ `user` - User (Internal) ■ `network` - Network (External) ■ `general` - General
`policy mode`	Auto-Topology assignment: ■ `on` - Auto-topology, or Manual override ■ `off` - Manual-General
`ssm 1 mode` `ssm 2 mode`	Distribution Mode assignment for SSM.
`ipv6 mode`	Shows the IPv6 status: ■ `on` - enabled ■ `off` - disabled
`l4_mode`	Shows the Layer 4 distribution status: ■ `on` - enabled ■ `off` - disabled
`40g mode`	Shows the QSFP port speed: ■ `on` - 1 x 40GbE ■ `off` - 4 x 10GbE
`matrix size`	Shows the size of the distribution matrix. The distribution matrix is a table that contains SGM IDs for traffic assignment.
`interface`	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 from a Maestro Security Group

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > 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] SG-s01-01 >
```

Example 2 - Verbose output of failed tests from a Maestro Security Group

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > 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] SG-s01-01 >
```

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 on a Maestro Security Group

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> set distribution l4-mode enabled
1_01:
success

1_02:
success
[Global] SG-s01-01>
```

Example 2 - Disable the Layer 4 Distribution Mode on a Maestro Security Group

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> set distribution l4-mode disabled
1_01:
success

1_02:
success
[Global] SG-s01-01>
```

Example 3 - Show the current Layer 4 Distribution Mode on a Maestro Security Group

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> show distribution l4-mode
1_01:
L4 Distribution: Enabled

1_02:
L4 Distribution: Enabled
[Global] SG-s01-01>
```

Example 4 - Show the current Layer 4 Distribution Mode on a Scalable Chassis

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > show distribution l4-mode
2_01:
L4 Distribution: Enabled
L4 Distribution IP mask: 0x0000007f
L4 Distribution port mask: 0x00000003
[Global] SG-s01-01 >
```

Setting the Administratively DOWN State on First Join

Note - This section applies to ElasticXL Cluster and Maestro.
For Scalable Chassis, see *"Setting the Administratively DOWN State on First Join in Dual Chassis" on page 387*.

Description

You can configure the Security Group to set a newly installed Security Group Member to be in the administratively DOWN state automatically.

The administrator can confirm that the Security Group Member is configured correctly before changing its state to UP.

Syntax

```
set cluster configuration high-availability down_on_first_join {0
| 1}
```

- 0 - Do **not** enable the administratively DOWN state automatically on a new Security Group Member for the first join.
- 1 - Enable the administratively DOWN state automatically on a new Security Group Member for the first join.

Procedure

Follow these steps to add a new Security Group Member to a Security Group in the administratively DOWN state:

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in.
3	If your default shell is the Expert mode (`/bin/bash`), then go to Gaia gClish: `gclish`
4	Enable the administratively DOWN state automatically on a new Security Group Member for the first join: `set cluster configuration high-availability down_on_first_join 1` To disable, run the same command with the value 0 (zero).

Step	Instructions
5	Install a new Security Appliance. **Important** - Do **not** run the Gaia First Time Configuration Wizard.
6	Add the new Security Appliance to the Security Group. ■ For ElasticXL Cluster, see *"Working with ElasticXL Cluster" on page 30*. ■ For Maestro, see *"Configuring Security Groups in Maestro" on page 98*.
7	Make sure the Security Group Member configuration is correct. Use one of these commands: ■ *"insights" on page 903* ■ *"hcp" on page 899*

8	Change the Security Group Member state to "UP" with this command:
	■ In the Expert mode:
	`cluster-cli set members-admin-state ids <SGM ID> up`
	See *"cluster-cli" on page 863*.
	■ In Gaia gClish:
	`set cluster members-admin-state ids <SGM ID> up`
	See *"set cluster members-admin-state" on page 933*.

NAT and the Correction Layer in the Gateway Mode

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 **General**.
Using NAT rule	■ Set the Distribution Mode to **User** for the networks hidden behind NAT. ■ Set the Distribution Mode to **Network** for the destination networks.

For information about the Distribution Mode, see *"Working with the Distribution Mode" on page 554*.

NAT and the Correction Layer in the VSNext / Traditional VSX Mode

In the VSNext / Traditional VSX Mode, the guidelines in NAT and the Correction Layer on a Security Gateway apply to each Virtual Gateway / Virtual System individually.

For best results, manage an entire session by a specified Virtual Gateway / Virtual System on the same Security Group Member.

When a Virtual Switch (junction) connects several Virtual Gateways / Virtual Systems, the same session can be handled by one Virtual Gateway / Virtual System on one Security Group Member, and by another Virtual Gateway / Virtual System on a different Security Group Member.

When a packet reaches a Virtual Gateway / Virtual System from a junction, the 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 Gateway / 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 the VSNext / Traditional VSX Mode:

NAT Rules	Guidelines
Not using NAT rules on any Virtual Gateway / Virtual System	Set the Distribution Mode to **General**.
Using NAT rule on at least one Virtual Gateway / Virtual System	■ On the Virtual Gateways / Virtual Systems that use NAT rules: • Set the Distribution Mode to **User** for the networks hidden behind NAT. • Set the Distribution Mode to **Network** for the destination networks. ■ On the remaining Virtual Gateways / Virtual Systems that do not use NAT rules: • Set the Distribution Mode to **User** for the internal networks. • Set the Distribution Mode to **Network** for the external networks.

For information about the Distribution Mode, see *"Working with the Distribution Mode" on page 554*.

Selecting Active Site in VSLS

Overview of VSLS

In the Traditional VSX mode, you can configure the Security Group to work in the Virtual System Load Sharing (VSLS) mode - see *"set cluster configuration high-availability" on page 925*.

In the VSLS mode, each Virtual System works as an independent cluster:

- One Site is Active for this Virtual System.
- One Site is Standby for this Virtual System.

Algorithm to Select an Active Site in VSLS

For each Virtual System independently, the VSLS mode selects the Active Site based on criteria in this order of priority:

1. **Availability of functional interfaces for the Virtual System:**

   The VSLS mode selects the Site with the most connected interfaces to be the Active Site.

2. **Availability of the Security Group Members in the state "UP":**

   If both Sites have the same number of connected interfaces, the VSLS mode uses this algorithm to select the Active Site:

   a. On each Site, get the number of the Security Group Members in the state "UP".

   b. Calculate the ratio:

   ```
   Ratio = [(the smaller number) / (the larger number)] x
   100%
   ```

   c. Select the Active Site based on the Ratio and the Threshold values:

   - If **Ratio < Threshold**, then select the Site with the most available Security Group Members to be the Active Site.
   - If **Ratio >= Threshold**, then skip to the next criterion.

   The default threshold value is 50%.

   The threshold determines the minimum required number of the Security Group Members in the state "UP" on a Site.

   If the ratio decreases below this threshold, then the VSLS mode performs the failover to the other Site.

Example:

a. Site 1 has two Security Group Members in the state "UP".

b. Site 2 has five Security Group Members in the state "UP".

c. Ratio = (2 / 5) x 100% = 40%

d. The ratio of 40% is lower than the default threshold of 50%.

e. The VSLS mode selects Site 2 as the Active Site.

You can control the threshold value with the kernel parameter "`fwha_mbs_vsls_chassis_sgm_ratio`":

a. Connect to the command line on the Security Group.

b. Get the current value:

- In Gaia gClish:

```
fw ctl get int fwha_mbs_vsls_chassis_sgm_ratio
```

- In the Expert mode:

```
g_allc fw ctl get int fwha_mbs_vsls_chassis_sgm_ratio
```

c. Configure the desired threshold value:

- In Gaia gClish:

```
update_conf_file fwkern.conf fwha_mbs_vsls_chassis_
sgm_ratio=<Value>
```

- In the Expert mode:

```
g_update_conf_file fwkern.conf fwha_mbs_vsls_chassis_
sgm_ratio=<Value>
```

3. **Virtual System reports a problem**

   When a Virtual System fails on the Active Site, the VSLS mode automatically performs the failover to the other Site, which becomes the new Active Site for this Virtual System.

4. **Primary Site**

   If none of the above criteria causes the VSLS mode to select an Active Site, the Primary Site automatically becomes the Active Site.

   To configure the Primary Site and the Secondary Site, see *"set cluster configuration high-availability" on page 925*.

Deploying a Security Group in Monitor Mode

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.

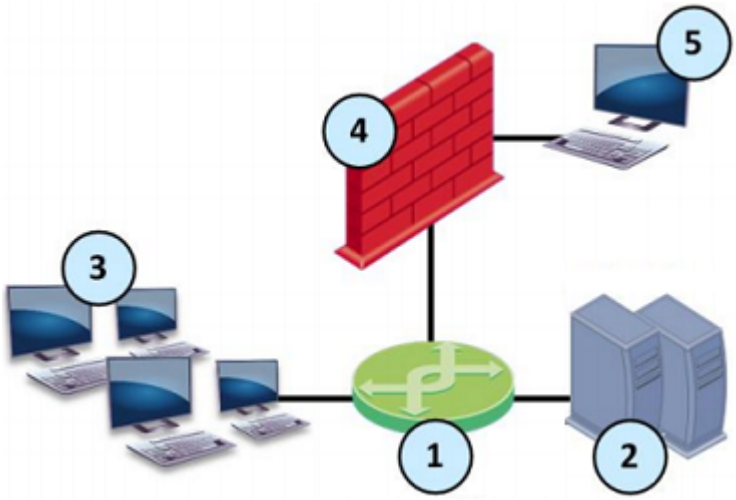
You can use the Monitor Mode:

- 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	These protections and features do **not** work: ■ The **SYN Attack** protection (SYNDefender). ■ The **Initial Sequence Number (ISN) Spoofing** protection. ■ The **Send error page** action in Web Intelligence protections. ■ Client and Server notifications about connection termination.
Application Control	Does **not** support UserCheck.
URL Filtering	Does **not** support UserCheck.
Data Loss Prevention	Does **not** support these: ■ UserCheck. ■ The **"Prevent"** and **"Ask User"** actions - these are automatically demoted to the **"Inform User"** action. ■ FTP inspection.
Identity Awareness	Does **not** support these: ■ Captive Portal. ■ Identity Agent.
Threat Emulation	Does **not** support these: ■ The Emulation Connection Prevent Handling Modes **"Background"** and **"Hold"**. See sk106119. ■ FTP inspection.
Content Awareness	Does **not** support the FTP inspection.
Anti-Bot	Fully supports the Monitor Mode.
Anti-Virus	Does **not** support the FTP inspection.
IPSec VPN	Does **not** support the Monitor Mode.
Mobile Access	Does **not** support the Monitor Mode.

Software Blade	Support for the Monitor Mode
Anti-Spam & Email Security	Does **not** support the Monitor Mode.
QoS	Does **not** 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 the '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 ElasticXL, see *"Working with ElasticXL Cluster" on page 30*.
   - For Maestro, see the *Maestro Getting Started Guide*
   - For Scalable Chassis, see the *Scalable Chassis Getting Started Guide* and *"Initial Software Installation and Configuration on Scalable Chassis" on page 294*.

Step	Instructions
1	Install the environment.
2	Configure the applicable Security Group and assign the applicable interface(s).
3	If you did not configure the **First Time Wizard settings** when you created a Security Group, you must run the Gaia First Time Configuration Wizard for the Security Group.

Step	Instructions
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

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: `https://<IP address of Gaia Management Interface>`
2	In the left navigation tree, click **Network Management** > **Network Interfaces**.
3	Select the applicable physical interface from the list and click **Edit**.
4	Select the **Enable** option to set the interface status to UP.
5	In the **Comment** field, enter the applicable comment text (up to 100 characters).
6	On the **IPv4** tab, select **Use the following IPv4 address**, but do **not** enter an IPv4 address.

Step	Instructions
7	On the **IPv6** tab, select **Use the following IPv6 address**, but do **not** enter an IPv6 address. **Important** - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the **Ethernet** tab: ■ Select **Auto Negotiation**, or select a link speed and duplex setting from the list. ■ In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC). **Caution** - 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. ■ In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ■ Select **Monitor Mode**.
9	Click **OK**.

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	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.
4	Examine the configuration and state of the applicable physical interface: `show interface <Name of Physical Interface>`

Step	Instructions

5	If the applicable physical interface has an IP address assigned to it, remove that IP address.
	■ To remove an IPv4 address:
	`delete interface <Name of Physical Interface> ipv4-address`
	■ To remove an IPv6 address:
	`delete interface <Name of Physical Interface> ipv6-address`

6	Enable the Monitor Mode on the physical interface: `set interface <Name of Physical Interface> monitor-mode on`
7	Configure other applicable settings on the interface in the Monitor Mode: `set interface <Name of Physical Interface> ...`
8	Examine the configuration and state of the Monitor Mode interface: `show interface <Name of Physical Interface>`
9	Save the configuration: `save config`

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 **Gateways & Servers**.

Step	Instructions
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter the applicable name for this Security Gateway object. b. In the **Gateway platform** field: ■ For Maestro, select: **Maestro** ■ For Scalable Chassis, select the supported model: • **44000 Appliances** • **64000 Appliances** c. In the **Gateway IP address** section, select **Static IP address** and configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** 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. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select the applicable option: ■ If you selected **Initiate trusted communication now**, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. ■ If you selected **Skip and initiate trusted communication later**, make sure to follow **Step 7**. b. Click **Next**.

Step	Instructions
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.
8	If during the Wizard Mode, you selected **Skip and initiate trusted communication later**: a. The **Secure Internal Communication** field shows **Uninitialized**. b. Click **Communication**. c. In the **Platform** field: ▪ For Maestro, select: **Maestro** ▪ For Scalable Chassis, select the supported model: • **44000 Appliances** • **64000 Appliances** d. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. e. Click **Initialize**. Make sure the **Certificate state** field shows **Established**. f. Click **OK**.
9	On the **Network Security** tab, make sure to enable only the Firewall Software Blade.
10	On the **Network Management** page: a. Click **Get Interfaces** > **Get Interfaces with Topology**. b. Confirm the interfaces information.
11	Click **OK**.
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

Configuring the Security Gateway 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 **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter the applicable name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** 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.

Step	Instructions
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field: ▪ For Maestro, select: **Maestro** ▪ For Scalable Chassis, select the supported model: • **44000 Appliances** • **64000 Appliances** c. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. d. Click **Initialize**. e. Click **OK**.

	If the **Certificate state** field does not show `Established`, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

Step	Instructions
8	In the **Platform** section, select the correct options: a. In the **Hardware** field: ▪ For Maestro, select: **Maestro** ▪ For Scalable Chassis, select the supported model: • **44000 Appliances** • **64000 Appliances** b. In the **Version** field, select **R82**. c. In the **OS** field, select **Gaia**.
9	On the **Network Security** tab, make sure to enable only the Firewall Software Blade. **Important** - Do **not** select anything on the **Management** tab.
10	On the **Network Management** page: a. Click **Get Interfaces** > **Get Interfaces with Topology**. b. Confirm the interfaces information.
11	Click **OK**.
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

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	Set the value of the kernel parameter **psl_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Passive Streaming Layer (PSL) Tap Mode:: `g_update_conf_file fwkern.conf psl_tap_enable=1`

Step	Instructions
4	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file fwkern.conf fw_tap_enable=1`
5	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$PPKDIR/conf/simkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file $PPKDIR/conf/simkern.conf fw_tap_enable=1`
6	Reboot the Security Group.
7	Connect to the command line on the Security Group.
8	Log in to the Expert mode.

9	Make sure the Security Group loaded the new configuration:
	`g_fw ctl get int psl_tap_enable`
	`g_fw ctl get int fw_tap_enable`

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 *Target*Domain Management Server that manages this Security Group.
2	In the top left corner, click **Menu > Global properties**.
3	From the left tree, click the **Stateful Inspection** pane and configure: a. In the **Default Session Timeouts** section: i. Change the value of the **TCP session timeout** from the default **3600** to **60** seconds. ii. Change the value of the **TCP end timeout** from the default **20** to **5** seconds. b. In the **Out of state packets** 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).
4	From the left tree, click the **Advanced** page > click the **Configure** button, and configure: a. Click **FireWall-1** > **Stateful Inspection**. b. Clear **reject_x11_in_any**. c. Click **OK** to close the **Advanced Configuration** window.
5	Click **OK** to close the **Global Properties** 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 **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>Create the Access Control rule that accepts all traffic:
<table>
<tr><th>No</th><th>Name</th><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th><th>Install On</th></tr>
<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>
</table></td></tr>
<tr><td>5</td><td>Best Practice
We recommend these Aggressive Aging settings for the most common TCP connections:
a. In the SmartConsole, click Objects menu > Object Explorer.
b. Open Services and select TCP.
c. Search for the most common TCP connections in this network.
d. Double-click the applicable TCP service.
e. From the left tree, click Advanced.
f. At the top, select Override default settings.
On Domain Management Server, select Override global domain settings.
g. Select Match for 'Any'.
h. In the Aggressive aging section:
Select Enable aggressive aging.
Select Specific and enter 60.
i. Click OK.
j. Close the Object Explorer.</td></tr>
<tr><td>6</td><td>Publish the SmartConsole session.</td></tr>
<tr><td>7</td><td>Install the Access Control Policy on the Security Gateway object.</td></tr>
</table>

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:

- For ElasticXL, see *"Working with ElasticXL Cluster" on page 30*.
- For Maestro, see the *Maestro Getting Started Guide*
- For Scalable Chassis, see the *Scalable Chassis Getting Started Guide* and *"Initial Software Installation and Configuration on Scalable Chassis" on page 294*.
- *R82 Gaia Administration Guide*.
- *R82 Security Management Administration Guide*.
- Applicable *Administration Guides* in sk181127 - Check Point Quantum R82 Release.

Configuring a Security Group in the 'Traditional 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 Maestro, see the *Maestro Getting Started Guide*
   - For Scalable Chassis, see the *Scalable Chassis Getting Started Guide* and *"Initial Software Installation and Configuration on Scalable Chassis" on page 294*.

Step	Instructions
1	Install the environment.
2	Configure the applicable Security Group.
3	If you did not configure the **First Time Wizard settings** when you created a Security Group, you must run the Gaia First Time Configuration Wizard for the Security Group.
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

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: `https://<IP address of Gaia Management Interface>`
2	In the left navigation tree, click **Network Management** > **Network Interfaces**.
3	Select the applicable physical interface from the list and click **Edit**.
4	Select the **Enable** option to set the interface status to UP.
5	In the **Comment** field, enter the applicable comment text (up to 100 characters).
6	On the **IPv4** tab, select **Use the following IPv4 address**, but do **not** enter an IPv4 address.
7	On the **IPv6** tab, select **Use the following IPv6 address**, but do **not** enter an IPv6 address. **Important** - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the **Ethernet** tab: ■ Select **Auto Negotiation**, or select a link speed and duplex setting from the list. ■ In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC). **Caution** - 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. ■ In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ■ Select **Monitor Mode**.
9	Click **OK**.

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	On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.
4	In the VSNext mode, go to the context of the applicable Virtual Gateway: `set virtual-system <ID>`
5	Examine the configuration and state of the applicable physical interface: `show interface <Name of Physical Interface>`

6	If the applicable physical interface has an IP address assigned to it, remove that IP address.
	■ To remove an IPv4 address:
	`delete interface <Name of Physical Interface> ipv4-address`
	■ To remove an IPv6 address:
	`delete interface <Name of Physical Interface> ipv6-address`

7	Enable the Monitor Mode on the physical interface: `set interface <Name of Physical Interface> monitor-mode on`
8	Configure other applicable settings on the interface in the Monitor Mode: `set interface <Name of Physical Interface> ...`
9	Examine the configuration and state of the Monitor Mode interface: `show interface <Name of Physical Interface>`

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	Set the value of the kernel parameter **psl_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Passive Streaming Layer (PSL) Tap Mode:: `g_update_conf_file fwkern.conf psl_tap_enable=1`
4	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file fwkern.conf fw_tap_enable=1`
5	Reboot the Security Group.
6	Connect to the command line on the Security Group.
7	Log in.

8	Make sure the Security Group loaded the new configuration:
	■ In Gaia gClish, run:
	`fw ctl get int psl_tap_enable`
	`fw ctl get int fw_tap_enable`
	■ In the Expert mode, run:
	`g_fw ctl get int psl_tap_enable`
	`g_fw ctl get int fw_tap_enable`

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 Legacy VSX Gateway object in SmartConsole**

   For the Traditional VSX mode, follow the steps below.

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Main* Domain Management Server that should manage this VSX Gateway.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new VSX Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✦) > **VSX** > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **VSX** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **VSX** > **Gateway** The **VSX Gateway Wizard** opens.

Step	Instructions
4	On the **VSX Gateway General Properties (Specify the object's basic settings)** page: a. In the **Enter the VSX Gateway Name** field, enter the applicable name for this VSX Gateway object. b. In the **Enter the VSX Gateway IPv4** field, enter the same IPv4 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. c. In the **Enter the VSX Gateway IPv6** field, enter the same IPv6 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. d. In the **Select the VSX Gateway Version** field, select **R82**. e. Click **Next**.
5	On the **VSX Gateway General Properties (Secure Internal Communication)** page: a. In the **Activation Key** field, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. b. In the **Confirm Activation Key** field, enter the same Activation Key again. c. Click **Initialize**. d. Click **Next**.

	If the **Trust State** field does not show **Trust established**, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, on the **VSX Gateway General Properties** page, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

Step	Instructions
6	On the **VSX Gateway Interfaces (Physical Interfaces Usage)** page: a. Examine the list of the interfaces - it must show all the physical interfaces on the Security Group. b. If you plan to connect more than one Virtual System directly to the same physical interface, you must select **VLAN Trunk** for that physical interface. c. Click **Next**.
7	On the **Virtual Network Device Configuration (Specify the object's basic settings)** page: a. You can select **Create a Virtual Network Device** and configure the first applicable Virtual Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. b. Click **Next**.
8	On the **VSX Gateway Management (Specify the management access rules)** page: a. Examine the default access rules. b. Select the applicable default access rules. c. Configure the applicable source objects, if needed. d. Click **Next**. **Important** - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.
9	On the **VSX Gateway Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
10	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

Step	Instructions
11	Install the default policy on the VSX Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the default policy for this VSX Gateway object. This policy is called: `<Name of VSX Gateway object>_VSX` c. Click **Install**.
12	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

5. **Configure the Legacy Virtual System object (and other Virtual Devices) in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or each *Target* Domain Management Server that should manage each Virtual Device.
2	Configure the applicable Virtual System (and other Virtual Devices) on this VSX Gateway. When you configure this Virtual System, for the Monitor Mode interface, add a regular interface. In the **IPv4 Configuration** section, enter a *random* IPv4 address. **Important** - This random IPv4 address must not conflict with existing IPv4 addresses on your network.
3	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

Step	Instructions
4	Disable the Anti-Spoofing on the interface that is configured in the Monitor Mode: a. In SmartConsole, open the Virtual System object. b. Click the **Topology** page. c. Select the Monitor Mode interface and click **Edit**. The **Interface Properties** window opens. d. Click the **General** tab. e. In the **Security Zone** field, select **None**. f. Click the **Topology** tab. g. In the **Topology** section, make sure the settings are **Internal (leads to the local network)** and **Not Defined**. h. In the **Anti-Spoofing** section, clear **Perform Anti-Spoofing based on interface topology**. i. Click **OK** to close the **Interface Properties** window. j. Click **OK** to close the **Virtual System Properties** window. k. The Management Server pushes the VSX Configuration.

6. **Configure the required Global Properties for the Legacy Virtual System in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target* Domain Management Server that manages this Virtual System.
2	In the top left corner, click **Menu > Global properties**.
3	From the left tree, click the **Stateful Inspection** pane and configure: a. In the **Default Session Timeouts** section: i. Change the value of the **TCP session timeout** from the default **3600** to **60** seconds. ii. Change the value of the **TCP end timeout** from the default **20** to **5** seconds. b. In the **Out of state packets** 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).
4	From the left tree, click the **Advanced** page > click the **Configure** button, and configure: a. Click **FireWall-1** > **Stateful Inspection**. b. Clear **reject_x11_in_any**. c. Click **OK** to close the **Advanced Configuration** window.

Step	Instructions
5	Click **OK** to close the **Global Properties** window.
6	Publish the SmartConsole session.

7. **Configure the required Access Control Policy for the Legacy Virtual System in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target*Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.
4	Create the **Access Control** rule that accepts all traffic:

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	**Best Practice** We recommend these **Aggressive Aging** settings for the most common TCP connections: a. In the SmartConsole, click **Objects** menu > **Object Explorer**. b. Open **Services** and select **TCP**. c. Search for the most common TCP connections in this network. d. Double-click the applicable TCP service. e. From the left tree, click **Advanced**. f. At the top, select **Override default settings**. On Domain Management Server, select **Override global domain settings**. g. Select **Match for 'Any'**. h. In the **Aggressive aging** section: Select **Enable aggressive aging**. Select **Specific** and enter **60**. i. Click **OK**. j. Close the **Object Explorer**.
6	Publish the SmartConsole session.
7	Install the Access Control Policy on the Virtual System object. a. Click **Install Policy**. b. In the **Policy** field, select the applicable policy for this Virtual System object. c. Click **Install**
8	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

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:

- For Maestro, see the *Maestro Getting Started Guide*
- For Scalable Chassis, see the *Scalable Chassis Getting Started Guide* and *"Initial Software Installation and Configuration on Scalable Chassis" on page 294*.
- *R82 Gaia Administration Guide*
- *R82 VSX Administration Guide*
- *R82 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:

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.</td></tr>
<tr><td>2</td><td>From the left navigation panel, click Security Policies > Threat Prevention.</td></tr>
<tr><td>3</td><td>Create the Threat Prevention rule that accepts all traffic:
<table>
<tr><th>Protected Scope</th><th>Protection/Site/File/Blade</th><th>Action</th><th>Track</th></tr>
<tr><td>*Any</td><td>-- N/A</td><td>Applicable Threat Prevention Profile</td><td>Log
Packet Capture</td></tr>
</table>
Notes:

We recommend the Optimized profile.
The Track setting Packet Capture is optional.

</td></tr>
<tr><td>4</td><td>Right-click the selected Threat Prevention profile and click Edit.</td></tr>
<tr><td>5</td><td>From the left tree, click the General Policy page and configure:
<ol type="a">
In the Blades Activation section, select the applicable Software Blades.
In the Activation Mode section:

In the High Confidence field, select Detect.
In the Medium Confidence field, select Detect.
In the Low Confidence field, select Detect.

</td></tr>
<tr><td>6</td><td>From the left tree, click the Anti-Virus page and configure:
<ol type="a">
In the Protected Scope section, select Inspect incoming and outgoing files.
In the File Types section:

Select Process all file types.
Optional: Select Enable deep inspection scanning (impacts performance).

Optional: In the Archives section, select Enable Archive scanning (impacts performance).

</td></tr>
</table>

Step	Instructions
7	From the left tree, click the **Threat Emulation** page > click **General** and configure: ▪ In the **Protected Scope** section, select **Inspect incoming files from the following interfaces** and from the menu, select **All**.
8	Configure other applicable settings for the Software Blades.
9	Click **OK**.
10	Install the Threat Prevention Policy on the Security Gateway object.

For more information:

See the *R82 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 **Manage & Settings > Blades**.
3	In the **Application Control & URL Filtering** section, click **Advanced Settings**. The **Application Control & URL Filtering Settings** window opens.
4	On the **General** page: ■ In the **Fail mode** section, select **Allow all requests (fail-open)**. ■ In the **URL Filtering** section, select **Categorize HTTPS websites**.
5	On the **Check Point online web service** page: ■ In the **Website categorization mode** section, select **Background**. ■ Select **Categorize social networking** widgets.
6	Click **OK** to close the **Application Control & URL Filtering Settings** window.
7	Install the Access Control Policy on the Security Gateway object.

For more information:

See the *R82 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 **Manage & Settings > Blades**.
3	In the **Data Loss Prevention** section, click **Configure in SmartDashboard**. The SmartDashboard window opens.
4	In SmartDashboard: a. Click the **My Organization** page. b. In the **Email Addresses or Domains** section, configure with full list of company's domains. There is no need to include subdomains (for example, `mydomain.com`, `mydomain.uk`). c. In the **Networks** section, select **Anything behind the internal interfaces of my DLP gateways**. d. In the **Users** section, select **All users**.
5	Click the **Policy** page. Configure the applicable rules: ■ In the **Data** column, right-click the pre-defined data types and select **Edit**. • On the **General Properties** page, in the **Flag** field, select **Improve Accuracy**. • In the **Customer Names** data type, we recommend to add the company's real customer names. ■ In the **Action** column, you must select **Detect**. ■ In the **Severity** column, select **Critical** or **High** in all applicable rules. ■ You may choose to disable or delete rules that are not applicable to the company or reduce the Severity of these rules. **Note** - Before you can configure the DLP rules, you must configure the applicable objects in SmartConsole.

Step	Instructions
6	Click the **Additional Settings > Protocols** page. Configure these settings: ■ In the **Email** section, select **SMTP (Outgoing Emails)**. ■ In the **Web** section, select **HTTP**. Do **not** configure the **HTTPS**. ■ In the **File Transfer** section, do **not** select **FTP**.
7	Click **Launch Menu > File > Update** (or press the **CTRL S** keys).
8	Close the SmartDashboard.
9	Install the Access Control Policy on the Security Gateway object.

10	Make sure the Security Group enabled the SMTP Mirror Port Mode:
	a. Connect to the command line on the Security Group.
	b. Log in to the Expert mode.
	c. Run this command:
	`dlp_smtp_mirror_port status`
	d. Make sure the value of the kernel parameter `dlp_force_smtp_kernel_inspection` is set to 1 (one).
	Run these two commands:
	`g_fw ctl get int dlp_force_smtp_kernel_inspection`
	`g_all grep dlp_force_smtp_kernel_inspection $FWDIR/boot/modules/fwkern.conf`

For more information:

See the *R82 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 sk100223: How to enable stripping of X-Forward-For (XFF) field.

Deploying a Security Group in Bridge Mode

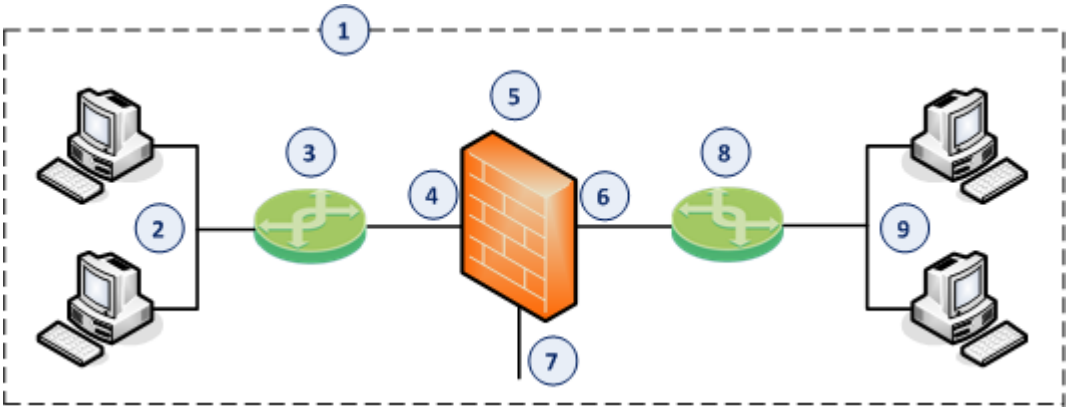
Introduction to Bridge Mode

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, `eth1-05`) on the Security Group in Bridge Mode.
5	Security Group in Bridge Mode.
6	Another bridged slave interface (for example, `eth1-07`) on the Security Group in Bridge Mode.
7	Dedicated Gaia Management Interface (for example, `eth1-Mgmt1`) 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 Monitor 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 (1)	Yes (1)
Application Control	Yes	Yes
HTTPS Inspection	Yes (2)	*No*
Identity Awareness	Yes (3)	*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
Threat Emulation - Remote emulation	Yes	Yes in Active/Active Bridge Mode *No* in Active/Standby Bridge Mode

Software Blade or Feature	Support of a Security Gateway in Bridge Mode	Support of VSX Virtual Systems in 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 sk89581)	*No* (see sk79700)
HTTP / HTTPS proxy	Yes	*No*
Security Servers - SMTP, HTTP, FTP, POP3	Yes	*No*
Client Authentication	Yes	*No*
User Authentication	Yes	*No*

Notes:

1. Does not support the Anti-Virus in Traditional Mode.
2. 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.
3. 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 ElasticXL, see *"Working with ElasticXL Cluster" on page 30*.
   - For Maestro, see the *Maestro Getting Started Guide*.
   - For Scalable Chassis, see the *Scalable Chassis Getting Started Guide* and *"Initial Software Installation and Configuration on Scalable Chassis" on page 294*.

Step	Instructions
1	Install the 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	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

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 **Network Management** > **Network Interfaces**.
2	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses.
3	Click **Add** > **Bridge**. To configure an existing Bridge interface, select the Bridge interface and click **Edit**.
4	On the **Bridge** tab, enter or select a **Bridge Group** ID (unique integer between 1 and 1024).
5	Select the interfaces from the **Available Interfaces** list and then click **Add**. **Notes:** ■ Make sure that the slave interfaces do not have any IP addresses or aliases configured. ■ Do **not** select the interface that you configured as Gaia Management Interface. ■ A Bridge interface in Gaia can contain only two slave interfaces.
6	On the **IPv4** tab, enter the IPv4 address and subnet mask. **Important** -
7	**Optional:** On the **IPv6** tab, enter the IPv6 address and mask length. **Important:** ■ First, you must enable the IPv6 Support and reboot (see the *R82 Gaia Administration Guide*).
8	Click **OK**.

Configuring the Bridge interface in Gaia gClish

Step	Instructions
1	Connect to the command line on the applicable Security Group.

Step	Instructions
2	Log in to Gaia Clish. On Scalable Platforms, go to Gaia gClish:Type `gclish` and press Enter.

3	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:
	`show interface <Name of Slave Interface> ipv4-address`
	`show interface <Name of Slave Interface> ipv6-address`

4	Add a new bridging group: `add bridging group <Bridge Group ID 0 - 1024>` **Note** - Do **not** change the state of bond interface manually using the "`set interface <Bridge Group ID> state`" command. This is done automatically by the bridging driver.

5	Add slave interfaces to the new bridging group:
	`add bridging group <Bridge Group ID> interface <Name of First Slave Interface>`
	`add bridging group <Bridge Group ID> interface <Name of Second Slave Interface>`
	Notes:
	■ Do **not** select the interface that you configured as Gaia Management Interface.
	■ Only Ethernet, VLAN, and Bond interfaces can be added to a bridge group.
	■ A Bridge interface in Gaia can contain only two slave interfaces.

Step	Instructions

6	Assign an IP address to the bridging group.
	Note - You configure an IP address on a Bridging Group in the same way as you do on a physical interface (see the *R82 Gaia Administration Guide*).
	■ To assign an IPv4 address, run:
	`set interface <Name of Bridging Group> ipv4-address <IPv4 Address> {subnet-mask <Mask> | mask-length <Mask Length>}`
	You can optionally configure the bridging group to obtain an IPv4 Address automatically.
	■ To assign an IPv6 address, run:
	`set interface <Name of Bridging Group> ipv6-address <IPv6 Address> mask-length <Mask Length>`
	You can optionally configure the bridging group to obtain an IPv6 Address automatically.
	Important - First, you must enable the IPv6 Support and reboot (see the *R82 Gaia Administration Guide*).

7	Save the configuration: `save config`

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 **Gateways & Servers**.

Step	Instructions
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter the applicable name for this Security Gateway object. b. In the **Gateway platform** field, select the applicable value: ■ For ElasticXL, select: ElasticXL ■ For Maestro, select: Maestro ■ For Scalable Chassis, select the supported model: **44000 Appliances** **64000 Appliances** c. In the **Gateway IP address** section, select **Static IP address** and configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** 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. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select the applicable option: ■ If you selected **Initiate trusted communication now**, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. ■ If you selected **Skip and initiate trusted communication later**, make sure to follow **Step 7**. b. Click **Next**.

Step	Instructions
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.
8	If during the Wizard Mode, you selected **Skip and initiate trusted communication later**: a. The **Secure Internal Communication** field shows **Uninitialized**. b. Click **Communication**. c. In the **Platform** field, select the applicable value: ▪ For ElasticXL, select: **ElasticXL** ▪ For Maestro, select: **Maestro** ▪ For Scalable Chassis, select the supported model: **44000 Appliances** **64000 Appliances** d. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. e. Click **Initialize**. Make sure the **Certificate state** field shows **Established**. f. Click **OK**.
9	On the **General Properties** page, on the **Network Security** tab, enable the applicable Software Blades. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 615*.
10	On the **Network Management** page, configure the **Topology** of the Bridge interface. **Notes:** ▪ If a Bridge interface connects to the Internet, then set the **Topology** to **External**. ▪ If you use this Bridge Security Gateway object in Access Control Policy rules with **Internet** objects, then set the **Topology** to **External**.

Step	Instructions
11	Click **OK**.
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 **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter the applicable name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** 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.

Step	Instructions
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field, select the applicable value: ▪ For ElasticXL, select: **ElasticXL** ▪ For Maestro, select: **Maestro** ▪ For Scalable Chassis, select the supported model: **44000 Appliances** **64000 Appliances** c. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. d. Click **Initialize**. e. Click **OK**.

	If the **Certificate state** field does not show `Established`, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

Step	Instructions
8	In the **Platform** section, select the correct options: a. In the **Hardware** field, select the applicable value: ▪ For ElasticXL, select: **ElasticXL** ▪ For Maestro, select: **Maestro** ▪ For Scalable Chassis, select the supported model: **44000 Appliances** **64000 Appliances** b. In the **Version** field, select **R82**. c. In the **OS** field, select **Gaia**.
9	On the **General Properties** page, on the **Network Security** tab, enable the applicable Software Blades. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 615*.
10	On the **Network Management** page, configure the **Topology** of the Bridge interface. **Notes:** ▪ If a Bridge interface connects to the Internet, then set the **Topology** to **External**. ▪ If you use this Bridge Security Gateway object in Access Control Policy rules with **Internet** objects, then set the **Topology** to **External**.
11	Click **OK**.
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 **Security Policies**.

Step	Instructions
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.
4	Create the applicable rules in the Access Control and Threat Prevention policies. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 615*.
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:

- For ElasticXL, see *"Working with ElasticXL Cluster" on page 30*.
- For Maestro - *Maestro Getting Started Guide*.
- For Scalable Chassis - *Scalable Chassis Getting Started Guide* and *"Initial Software Installation and Configuration on Scalable Chassis" on page 294*.
- *R82 Gaia Administration Guide*.
- *R82 Security Management Administration Guide*.
- Applicable *Administration Guides* in sk181127 - Check Point Quantum R82 Release.

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 `/etc/rc.d/init.d/network` file: `cp -v /etc/rc.d/init.d/network{,_BKP}`
4	Edit the current `/etc/rc.d/init.d/network` file: `vi /etc/rc.d/init.d/network`

5	After the line:
	`./etc/init.d/functions`
	Add this line:
	`/sbin/sysctl -w net.bridge.bpdu_ forwarding=0`

6	Save the changes in the file and exit the editor.
7	Reboot the Security Group: `reboot -b all`
8	Connect to the command line on the applicable Security Group.
9	Log in to the Expert mode.

Step	Instructions

10	Make sure the new configuration is loaded:
	`sysctl net.bridge.bpdu_forwarding`
	The expected output:
	`net.bridge.bpdu_forwarding = 0`

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 in Bridge Mode

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	On the Security Group, configure the value of the kernel parameter `fwaccept_unknown_protocol` to 0.
	a. Connect to the command line on the Security Group.
	b. Log in to the Expert mode.
	c. Configure the value of the kernel parameter `fwaccept_unknown_protocol` to 0:
	`g_update_conf_file fwkern.conf fwaccept_unknown_protocol=0`
	d. Reboot the Security Group.
	If the reboot is not possible at this time, then:
	■ Run this command to make the required change:
	`g_fw ctl set int fwaccept_unknown_protocol 0`
	■ Run this command to make sure the required change was accepted:
	`g_fw ctl get int fwaccept_unknown_protocol`

Step	Instructions

2	On the Management Server, edit the applicable `user.def` file.
	Note - For the list of `user.def` files, see sk98239.
	a. Back up the current applicable `user.def` file.
	b. Edit the current applicable `user.def` file.
	c. Add these directives:
	■ `allowed_ethernet_protocols` - contains the EtherType numbers (in Hex) of protocols to accept
	■ `dropped_ethernet_protocols` - contains the EtherType numbers (in Hex) of protocols to drop
	Example
	`$ifndef __user_def__`
	`$define __user_def__`
	
	`\\`
	`\\ User defined INSPECT code`
	`\\`
	
	`allowed_ethernet_protocols={`
	`<0x0800,0x86DD,0x0806>);dropped_ethernet_protocols={`
	`<0x8137,0x8847,0x9100> );`
	
	`endif /*__user_def__*/`
	For the list of EtherType numbers, see http://standards-oui.ieee.org/ethertype/eth.csv.
	d. Save the changes in the file and exit the editor.

3	In SmartConsole, install the Access Control Policy on the Security Gateway object.

System Optimization on Security Groups

This section describes some optimization steps you can take on Security Groups.

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 *R82 Performance Tuning Administration Guide*.

Firewall Connections Table Size for Traditional VSX Gateway

This information applies only to a Security Group configured in the Traditional VSX mode (does **not** apply to the VSNext mode).

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 **Gateways & Servers**.
3	Open the Virtual System object.
4	From the left tree, click **Optimizations**.
5	In the **Calculate the maximum limit for concurrent connections** section, select **Manually**.
6	Enter or select a value.
7	Click **OK**.
8	Install the Access Control Policy on the Virtual System object.

System Monitoring on Security Groups

This section provides monitoring commands on Security Groups.

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
Header	This view shows the time the statistics in the third view are collected. It updates when you refresh the statistics.
Navigation	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.
View	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 **Overview** view.
Enter	Changes to the **View Mode**. On a menu with sub-menus, the **Enter** key moves you to the lowest level sub-menu.
Esc	Returns to the **Menu Mode**.
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: `cpview_<ID of the cpview process>.cap<Number of the capture>`
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

Working with SNMP

You can use SNMP to monitor these:

Where to Configure?	What to Monitor?	How to Monitor?
■ Orchestrator	Orchestrator	*"SNMP for Maestro Orchestrators" on page 644*
■ ElasticXL ■ Maestro ■ Scalable Chassis	Entire Security Group	*"SNMP for Security Groups" on page 647*
■ ElasticXL ■ Maestro ■ Scalable Chassis	Specific Security Group Members	*"SNMP for Security Group Members" on page 670*

SNMP for Maestro Orchestrators

You can use SNMP to monitor different aspects of the Maestro Orchestrator:

- Software versions
- Key performance indicators

Notes:

- Hardware monitoring with SNMP is not supported on Orchestrators..
- For SNMP monitoring of Security Groups, see *"SNMP for Security Groups" on page 647*.
- For SNMP monitoring of Security Group Members, see *"SNMP for Security Group Members" on page 670*.

Prerequisites

Step	Instructions
1	On the Maestro Orchestrator, in Gaia Portal or Gaia gClish: a. Enable the SNMP Agent. b. Configure SNMP settings. **Best Practice** - Use only SNMP v3. See the *R82 Gaia Administration Guide* > Chapter "System Management" > Section "SNMP".
2	Upload these Check Point MIB files from the Security Group to your third-party SNMP monitoring software: ■ The SNMP MIB file: `$CPDIR/lib/snmp/chkpnt.mib` ■ The SNMP Trap MIB file: `$CPDIR/lib/snmp/chkpnt-trap.mib` (The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.)

Supported SNMP OIDs for Maestro Orchestrators

Only these OID 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 Maestro Orchestrators

Only these OID 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.

SNMP for Security Groups

Important - This topic described the steps to get aggregated SNMP data from all Security Group Members.
To get SNMP data from a specific Security Group Member, see *"SNMP for Security Group Members" on page 670*.

You can use SNMP to monitor different aspects of a Security Group, including:

- Software versions
- Hardware status
- Key performance indicators
- High Availability status

Prerequisites

Step	Instructions
1	On the Security Group, in Gaia Portal or Gaia gClish: a. Enable the SNMP Agent. b. Configure SNMP settings. **Best Practice** - Use only SNMP v3. See the *R82 Gaia Administration Guide* > Chapter "System Management" > Section "SNMP".

2	Upload these Check Point MIB files from the Security Group to your third-party SNMP monitoring software:
	■ The SNMP MIB file:
	`$CPDIR/lib/snmp/chkpnt.mib`
	■ The SNMP Trap MIB file:
	`$CPDIR/lib/snmp/chkpnt-trap.mib`
	(The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.)

Supported SNMP OIDs for Security Groups

Supported SNMP OIDs from the `$CPDIR/lib/snmp/chkpnt.mib` file

Explanation

OID Name	OID Numerical Value	OID Description
`asg`	`1.3.6.1.4.1.2620.1.48`	Main OID branch.
`asgProductName`	`1.3.6.1.4.1.2620.1.48.1`	Product name.
`asgVer`	`1.3.6.1.4.1.2620.1.48.2`	Build version.
`asgKernelVer`	`1.3.6.1.4.1.2620.1.48.3`	Kernel version.
`asgBuildNum`	`1.3.6.1.4.1.2620.1.48.4`	Build number.
`asgMaximumBladesPerChassis`	`1.3.6.1.4.1.2620.1.48.7`	Maximum number of Security Group Members per Site.
`asgActiveBladesBitmask`	`1.3.6.1.4.1.2620.1.48.8`	Bitmask of active Security Group Members: ■ Site 1 - 16 Least Significant Bits ■ Site 2 - 16 Most Significant Bits Example: `asgActiveBladesBitmask = 00030002` means that ■ The Security Group Member 2 is active on Site 1. ■ The Security Group Members 1 and 2 are active on Site 2.

OID Name	OID Numerical Value	OID Description
`asgInstalledBladesBitmask`	`1.3.6.1.4.1.2620.1.48.9`	Bitmask of installed Security Group Members: ■ Site 1 - 16 Least Significant Bits ■ Site 2 - 16 Most Significant Bits Example: `asgInstalledBladesBitmask = 00030002` means that ■ The Security Group Member 2 is installed on Site 1. ■ The Security Group Members 1 and 2 are installed on Site 2.
`asgInstalled`	`1.3.6.1.4.1.2620.1.48.10`	Date and time of the software installation.
`asgSystemUp`	`1.3.6.1.4.1.2620.1.48.11`	Time elapsed since the last startup.
`asgEvent`	`1.3.6.1.4.1.2620.1.48.12`	A string that contains the last SNMP Trap sent.
`asgStatusCode`	`1.3.6.1.4.1.2620.1.48.13`	Status code.
`asgStatShort`	`1.3.6.1.4.1.2620.1.48.14`	Status short description.
`asgStatLong`	`1.3.6.1.4.1.2620.1.48.15`	Status long description.

OID Name	OID Numerical Value	OID Description
`asgSecureXLStatusBitmask`	`1.3.6.1.4.1.2620.1.48.16`	Bitmask of the SecureXL status: ■ Site 1 - 16 Least Significant Bits ■ Site 2 - 16 Most Significant Bits Example: `asgSecureXLStatusBitmask = 00030002` means that ■ SecureXL is enabled on the Security Group Member 2 on Site 1. ■ SecureXL is enabled on the Security Group Members 1 and 2 on Site 2.
`asgAttachedBladesBitmask`	`1.3.6.1.4.1.2620.1.48.17`	Bitmask of attached Security Group Members: ■ Site 1 - 16 Least Significant Bits ■ Site 2 - 16 Most Significant Bits Example: `asgAttachedBladesBitmask = 00030002` means that ■ The Security Group Member 2 is attached on Site 1. ■ The Security Group Members 1 and 2 are attached on Site 2.

OID Name	OID Numerical Value	OID Description
asgIPv4PerformanceCounters	1.3.6.1.4.1.2620.1.48.20	Various IPv4 performance counters: ■ Throughput ■ Connection rate ■ Packet rate
asgIPv6PerformanceCounters	1.3.6.1.4.1.2620.1.48.21	Various IPv6 performance counters: ■ Throughput ■ Connection rate ■ Packet rate
asgHwMonitoring	1.3.6.1.4.1.2620.1.48.22	Hardware sensors (only on Scalable Chassis).
asgResourceTable	1.3.6.1.4.1.2620.1.48.23	Table that contains information and measured values of memory and disk partitions.
asgProtocolTraffic	1.3.6.1.4.1.2620.1.48.24	Various counters for processed traffic protocols: ■ Protocol name ■ Total number of processed connections ■ Total number of processed packets ■ Total number of processed bytes

OID Name	OID Numerical Value	OID Description
asgProtocolTraffic	1.3.6.1.4.1.2620.1.48.25	Various counters for processed traffic ports (services): ■ Service name ■ Total number of processed connections ■ Total number of processed packets ■ Total number of processed bytes
asgSetup	1.3.6.1.4.1.2620.1.48.26	Network information: ■ Indexes of interfaces ■ Names of interfaces ■ IPv4 addresses of interfaces ■ IPv6 addresses of interfaces ■ MAC addresses of interfaces ■ State of interfaces ■ Speed of interfaces (not supported on Maestro) ■ MTU of interfaces ■ Duples of interfaces ■ Total received data through interfaces ■ Total transmitted data through interfaces
asgProblemTable	1.3.6.1.4.1.2620.1.48.27	

OID Name	OID Numerical Value	OID Description
asgChassisInfo	1.3.6.1.4.1.2620.1.48.28	Information about the Dual Site: ■ Single Site or Dual Site ■ High Availability Mode- "Primary Up" or "Active Up". ■ State of the synchronization between the Sites ■ Parameters - status, grade, unique IP address ■ Information about Security Group Members ■ Information about factors: 1. SGM 2. Failover 3. Port (Standard Priority) 4. Port (High Priority) 5. Sync between Chassis Ratio 6. Fans 7. SSMs 8. CMMs 9. PSUs 10. Pingable Hosts ■ Information about port priority
asgCoresUtilTable	1.3.6.1.4.1.2620.1.48.29	CPU utilization (in %) on each Security Group Member.

OID Name	OID Numerical Value	OID Description
`asgVSX`	`1.3.6.1.4.1.2620.1.48.30`	Information about Traditional VSX mode for each Virtual System and in total: ■ VSLS state ■ Number of connections ■ Memory utilization ■ CPU utilization ■ Number of packets ■ Throughput ■ Connection rate
`asgDiagnostic`	`1.3.6.1.4.1.2620.1.48.31`	List of diagnostic tests and their result. **Best Practice** - Run the "`insights`" command (*"insights" on page 903*) or the "`hcp`" command (*"hcp" on page 899*) on a regular basis.

Supported SNMP Trap OIDs for Security Groups

Note - The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.

Supported SNMP Trap OIDs from the `$CPDIR/lib/snmp/chkpnt-trap.mib` file

Explanation

OID Name	OID Numerical Value	OID Description
`asgTrap`	`1.3.6.1.4.1.2620.1.2001`	Main OID branch.
`asgTrapInfo`	`1.3.6.1.4.1.2620.1.2001.0`	Information about the SNMP Trap message: ■ Site ID (Chassis ID) ■ Security Group Member ID (Blade ID) ■ Alert message text ■ Alert message priority ■ SNMP OID that triggered the alert ■ Security Group Member's serial number ■ Security Group Member's CPU core ID ■ SNMP trap category

OID Name	OID Numerical Value	OID Description
asgTrapHA	1.3.6.1.4.1.2620.1.2001.1	In Dual Site: ■ State of Site (Chassis state) ■ State of a Security Group Member (Blade state) ■ Cluster problem status ■ Monitor state
asgTrapNet	1.3.6.1.4.1.2620.1.2001.2	Information about an interface: ■ Interface Status Alert ■ Administrative Status Alert
asgTrapDisk	1.3.6.1.4.1.2620.1.2001.3	Information about storage devices: ■ Disk partition is full ■ State of a RAID volume ■ State of a RAID disk
asgTrapCPU	1.3.6.1.4.1.2620.1.2001.4	Information about CPU cores: ■ Utilization of CPU core ■ Number of interrupts in a CPU core
asgTrapMemory	1.3.6.1.4.1.2620.1.2001.5	Information about memory: ■ Utilization of swap memory ■ Utilization of real memory

OID Name	OID Numerical Value	OID Description
asgTrapCplic	1.3.6.1.4.1.2620.1.2001.6	Information about a license
asgTrapHWSensor	1.3.6.1.4.1.2620.1.2001.7	Information about hardware sensors (only on Scalable Chassis): ■ Temperature ■ Fan speed ■ Voltage ■ SSM ■ CMM

OID Name	OID Numerical Value	OID Description
asgTrapPerf	1.3.6.1.4.1.2620.1.2001.8	Information about performance: ■ Connection rate (conn/sec) on each Security Group Member ■ Number of concurrent connections on each Security Group Member ■ Total number of concurrent connections on a Security Group ■ Connection rate (conn/sec) on a Security Group ■ Throughput (bits/sec) on each Security Group Member ■ Total throughput (bits/sec) on a Security Group ■ Packet rate (packets/sec) on each Security Group Member ■ Total packet rate (packets/sec) on a Security Group

OID Name	OID Numerical Value	OID Description
asgTrapGeneral	1.3.6.1.4.1.2620.1.2001.10	Additional information: ■ Route inconsistency ■ Periodic system diagnostics ■ State of pingable hosts ■ Memory leak detection reached a threshold ■ Activation of the SecureXL Accelerated SYN Defender ■ State of a port in an LSP Group changed

Supported additional SNMP Trap OIDs

Explanation

- Syntax in Gaia gClish on a Security Group to see all supported thresholds:

  ```
  show cluster alert_threshold[Esc][Esc]
  ```

- Syntax in Gaia gClish on a Security Group to see the description of a threshold:

  ```
  show cluster alert_threshold <Threshold Name>[Space]
  [Shift+?]
  ```

- Syntax in Gaia gClish on a Security Group to see the current threshold value:

  ```
  show cluster alert_threshold <Threshold Name>
  ```

- Syntax in Gaia gClish on a Security Group to configure a threshold value:

  ```
  set cluster alert_threshold <Threshold Name> <Threshold
  Value>
  ```

SNMP Trap Name	SNMP Trap Description
`AsgDiagAllTests`	Sends an SNMP Trap with the results of all applicable tests.
`BladeStateEvent`	The state of a Security Group Member changed.
`ChassisStateEvent`	The state of a Site changed.

SNMP Trap Name	SNMP Trap Description
`ConcurrConnEvent`	The number of concurrent connections is above or lower than the configured thresholds. Thresholds: ■ `concurr_conn_threshold_high` High threshold for concurrent connections, per CPU Default: 2,000,000 ■ `concurr_conn_threshold_low_ratio` Low threshold for concurrent connections, as percentage from the high threshold Default: 80% ■ `concurr_conn_total_threshold_high` High threshold for total concurrent connections, system-wide Default: 20,000,000 ■ `concurr_conn_total_threshold_low_ratio` Low threshold for system-wide total concurrent connections, as percentage from the high threshold Default: 80%

SNMP Trap Name	SNMP Trap Description
`ConnRateEvent`	The rate of connections is above or lower than the configured thresholds. Thresholds: ■ `conn_rate_threshold_high` High threshold for connection rate (conn/sec), per CPU Default: 30,000 ■ `conn_rate_threshold_low_ratio` Low threshold for connection rate (conn/sec), as percentage from the high threshold Default: 80% ■ `conn_rate_total_threshold_high` High threshold for total connection rate (conn/sec), system-wide Default: 300,000 ■ `conn_rate_total_threshold_low_ratio` Low threshold for system-wide total connection rate (conn/sec), as percentage from the high threshold Default: 80%
`CPUUsagePeak`	The CPU utilization is above or lower than the configured thresholds. Thresholds: ■ `cpu_load_threshold_perc_high` High threshold for CPU utilization Default: 75% ■ `cpu_load_threshold_perc_low_ratio` Low threshold for CPU utilization, as percentage from the high threshold Default: 80%

SNMP Trap Name	SNMP Trap Description
`HdUtilEvent`	The hard disk utilization is above or lower than the configured thresholds. Thresholds: ■ `hd_util_threshold_perc_high` High threshold for hard drive utilization Default: 80% ■ `hd_util_threshold_perc_low_ratio` Low threshold for hard drive utilization, as percentage from the high threshold Default: 80%
`HWMonitorFansEvent`	Applies only to Scalable Chassis. One of these: ■ The state of a Fan changed. ■ The Fan speed is above or lower than the configured threshold.
`HWMonitorPowerEvent`	Applies only to Scalable Chassis. One of these: ■ The state of a Power Supply Unit changed. ■ The Power Supply Unit voltage is above or lower than the configured threshold.
`HWMonitorSSMEvent`	Applies only to Scalable Chassis. One of these: ■ The state of a Security Switch Module (SSM) changed. ■ The state of a Security Switch Module (SSM) is "`Management Loss`" (see sk145792).
`HWMonitorSystemManagerEvent`	Applies only to Scalable Chassis. An event occurred in a Chassis Management Module (CMM).

SNMP Trap Name	SNMP Trap Description
`HWMonitorTemperatureEvent`	Applies only to Scalable Chassis. One of these: ■ The value of the CPU temperature changed. ■ The CPU temperature value is above or lower than the configured threshold.
`LspPortEvent`	The state of a port that is configured in a Link State Propagation (LSP) Group changed. See: ■ *"Configuring Link State Propagation (LSP) on a Maestro Orchestrator" on page 258* ■ *"Configuring Link State Propagation (LSP) on Scalable Chassis" on page 368*
`MemoryLeakDetectEvent`	A memory leak was detected.
`MemUtilEvent`	The memory utilization is above or lower than the configured thresholds. Thresholds: ■ `mem_util_threshold_perc_high` High threshold for memory utilization Default: 50% ■ `mem_util_threshold_perc_low_ratio` Low threshold for memory utilization, as percentage from the high threshold Default: 80%
`MonitorStateEvent`	■ In the VSNext mode: The state of a monitored Virtual Gateway changed. ■ In the Traditional VSX mode: The state of a monitored Virtual System changed.

SNMP Trap Name	SNMP Trap Description
`PacketRateEvent`	The packet rate is above or lower than the configured thresholds. Thresholds: ■ `packet_rate_threshold_high` High threshold for packet rate (packets/sec), per CPU Default: 1,000,000 ■ `packet_rate_threshold_low_ratio` Low threshold for packet rate (packets/sec), as percentage from the high threshold Default: 80% ■ `packet_rate_total_threshold_high` High threshold for total packet rate (packets/sec), system-wide Default: 10,000,000 ■ `packet_rate_total_threshold_low_ratio` Low threshold for system-wide total packet rate (packets/sec), as percentage from the high threshold Default: 80%
`PortStatusChangeEvent`	The state of a port link changed.

SNMP Trap Name	SNMP Trap Description
`ThroughputEvent`	The throughput is above or lower than the configured thresholds. Thresholds: ■ `throughput_threshold_high` High threshold for throughput (bits/sec), per CPU Default: 3,000,000,000 ■ `throughput_threshold_low_ratio` Low threshold for throughput (bits/sec), as percentage from the high threshold Default: 80% ■ `throughput_total_threshold_high` High threshold for total throughput (bits/sec), system-wide Default: 30,000,000,000 ■ `throughput_total_threshold_low_ratio` Low threshold for system-wide total throughput (bits/sec), as percentage from the high threshold Default: 80%

SNMP Monitoring of Security Groups in the VSNext / Traditional VSX Mode

For more information, see the:

- *R82 Gaia Administration Guide*
- *R82 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: ■ throughput ■ pps ■ cps ■ concurrent connections
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: ■ throughput ■ cps ■ pps ■ concurrent connections ■ SecureXL CPU usage (avg / min / max) ■ Firewall CPU usage (avg / min / max)

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	
Sensors on every Chassis	Table	1.3.6.1.4.1.2620.1.48.22.1.1	**Note** - Available only on Scalable Chassis. Status details of: ■ Fans ■ SSMs ■ CPU temperature ■ CMM ■ PSUs ■ PSU Fans
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	

SNMP for Security Group Members

Important - This topic described the steps to get SNMP data from a specific Security Group Member.
To get aggregated SNMP data from all Security Group Members, see *"SNMP for Security Groups" on page 647*.

Background

By default, when you query a Security Group over SNMP, you can get only these data:

- SNMP data only from the Security Group Member that accepted the SNMP connections:
  - If the connection arrives at the "**Mgmt**" port assigned to the Security Group, then the Single Management Object (SMO) Security Group Member accepts it.
  - If the connection arrives at one of the Data ports assigned to the Security Group, then one of the Security Group Members accepts it (based on the Source IP Address / Port and the Destination IP Address / Port).
- Aggregated SNMP data from all Security Group Members (with the SNMP OID branch "`asg`").

To get SNMP data from a specific Security Group Member , we use the SNMPv3 proxy feature "`ContextName`".

SNMP flow:

1. An SNMP client sends the required SNMP query to the Security Group for the specified Security Group Member.
2. A Security Group Member that accepts the SNMP connection forwards it to the specified Security Group Member over the internal synchronization network.
3. The specified Security Group Member responds with the SNMP data (over the internal synchronization network) to the Security Group Member that accepted the SNMP connection.
4. The Security Group Member that accepted the SNMP connection, responds with the SNMP data to the SNMP client.

The SNMP Client is unaware of this SNMP proxy feature on the Security Group Member. From the SNMP Client point of view, the SNMP connection is established directly the specified Security Group Member.

Limitations

- This feature supports a maximum of 10 Security Group Members in a Security Group.
- In the Traditional VSX mode, it is not supported to send SNMP queries to the IP addresses of Virtual Systems other than VS0 (the SNMP VS mode "`vs-direct-access`" is not supported). This is because the internal synchronization interface is not available in the context of Virtual Systems other than VS0.

Prerequisites

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>On the Security Group, in Gaia Portal or Gaia gClish:

a. Enable the SNMP Agent.
b. Configure an SNMP v3 user with these settings:
i. Security Level "<code>authPriv</code>"
ii. Authentication Protocol and Authentication Pass phrase
iii. Privacy Protocol and Privacy Pass phrase

See the <i>R82 Gaia Administration Guide</i> > Chapter "System Management" > Section "SNMP".

Important - In the VSNext / Traditional VSX mode, this SNMP v3 user must have access to the required Virtual Gateways / Legacy Virtual Systems:
<code>set snmp usm user <<i>SNMPv3 USM User</i>> vsid <<i>Range of VSIDs</i>></code></td></tr>
<tr><td>2</td><td>Upload these Check Point MIB files from the Security Group to your third-party SNMP monitoring software:

■ The SNMP MIB file:
<code>$CPDIR/lib/snmp/chkpnt.mib</code>
■ The SNMP Trap MIB file:
<code>$CPDIR/lib/snmp/chkpnt-trap.mib</code>
(The <code>/etc/snmp/GaiaTrapsMIB.mib</code> file is not supported.)</td></tr>
<tr><td>3</td><td>In the Access Control policy, configure this explicit rule for the SNMP traffic (UDP port 161) in the internal synchronization network and install this policy on the applicable Security Gateway object for this Security Group:

<table>
<tr><th>Name</th><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th><th>Install On</th></tr>
<tr><td>SNMP for Security Group Members</td><td>Network Object for the IP address 192.0.2.0 / 24</td><td>Network Object for the IP address 192.0.2.0 / 24</td><td><code>Any</code></td><td><code>snmp</code></td><td><code>Accept</code></td><td><code>Log</code> or <code>None</code></td><td><code>Policy Targets</code></td></tr>
</table>
</td></tr>
</table>

Enabling SNMP for Specific Security Group Members

Procedure

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia gClish.
3	Enable SNMP per Security Group Member: a. With the Context Distribution mode. b. For the applicable SNMPv3 USM user. `set snmp snmp-per-member state on mode ctx-dist user <SNMPv3 USM User>` **Notes:** ■ You must enter the SNMPv3 USM user explicitly. This command does not suggest a list of configured SNMPv3 USM users. ■ The command must return this line for each Security Group Member: "`SNMP Per Member configuration finished successfully`"
4	Examine the state of the SNMP per Security Group Member feature: `show snmp snmp-per-member state` The command must return "`on`" for each Security Group Member.

5	Run the applicable SNMPv3 query:
	`snmpwalk -v 3 -u <SNMPv3 USM User> -l <AuthenticationLevel> -a <AuthenticationProtocol> -A <AuthenticationPhrase> -x PrivacyProtocol -X PrivacyPhrase <IP Address of Security Group> -n <Name of SNMPv3 Context for Security Group Member> <SNMP OID>`
	Example for the Security Group Member 1_2 and the Check Point SNMP OID "`svn.sysInfo.sysDescr`":
	`snmpwalk -v 3 -u MyUsmUser -l AuthPriv -a SHA256 -A MyUsmAuthPhrase -x AES256 -X MyUsmPrivacyPhrase 172.16.103.220 -n MEMBER1_2 .1.3.6.1.4.1.2620.1.6.23.1.0`

CLI Syntax for SNMP configuration

```
set snmp snmp-per-member
      state on mode <Mode> user <SNMPv3 USM User>
      state off
```

```
show snmp snmp-per-member {mode | state | user}
```

CLI Parameters for SNMP configuration

Parameter	Description
`mode <Mode>`	Specifies the mode for the SNMP per Security Group Member feature. Press the TAB key to see the available options.
`user <SNMPv3 USM User>`	Specifies the SNMPv3 USM User you created in Gaia OS. See *"Prerequisites" on page 672*.

CLI Syntax for SNMP query (based on 'snmpwalk')

```
snmpwalk -v 3 -u <SNMPv3 USM User> -l <AuthenticationLevel> -a
<AuthenticationProtocol> -A <AuthenticationPhrase> -x
<PrivacyProtocol> -X <PrivacyPhrase> <IP Address of Security
Group> -n <Name of SNMPv3 Context for Security Group Member> <SNMP
OID>
```

CLI Parameters for SNMP query

Parameter	Description
`-u <SNMPv3 USM User>`	Specifies the SNMPv3 USM User you created in Gaia OS. See *"Prerequisites" on page 672*.
`-l <AuthenticationLevel>`	Specifies the SNMPv3 Authentication Level. This feature requires "`AuthPriv`".
`-a <AuthenticationProtocol>`	Specifies the SNMPv3 Authentication Protocol.
`-A <AuthenticationPhrase>`	Specifies the SNMPv3 Authentication Passphrase.
`-x <PrivacyProtocol>`	Specifies the SNMPv3 Privacy Protocol.
`-X <PrivacyPhrase>`	Specifies the SNMPv3 Privacy Passphrase.
`<IP Address of Security Group>`	Specifies the IP address of the Security Group / ElasticXL Cluster.

Parameter	Description
`-n <Name of SNMPv3 Context for Security Group Member>`	Specifies the Security Group Member to query. You must use the correct string as listed below. On Site 1: ■ `MEMBER1_1` ■ `MEMBER1_2` ■ ... ■ `MEMBER1_10` On Site 2: ■ `MEMBER2_1` ■ `MEMBER2_2` ■ ... ■ `MEMBER2_10` **Important** - The parameter "`-n <Name of SNMPv3 Context for Security Group Member>`" does not support the SMO Security Group Member, regardless from which Security Group Member you run this command.
`<SNMP OID>`	Specifies the SNMP OID to query.

Files

- `/var/log/snmp_per_member.log`

  Log file.

- `/etc/snmp/scalable_platform.conf`

  Internal configuration file.

  Important:
  - Do **not** edit this file manually.
    Use only the Gaia gClish command "`set snmp snmp-per-member`".
  - Gaia OS also saves the required settings in its database.
    To see these settings, run in the Expert mode:
    `dbget -rva snmp:per_member`

Monitoring Performance

To monitoring the performance, use these commands in Gaia gClish:

- *"insights" on page 903*
- *"show cluster info" on page 967*
  - `show cluster info overview [live] [format json]`
  - `show cluster info cpu [live] [format json]`
  - `show cluster info throughput [live] [format json]`
- *"asg_blade_stats" on page 712*

Monitoring Traffic

To monitor traffic in your Security Group, use these commands.

To show information about connections:

- *"asg_conns" on page 725*
- *"insights" on page 903*
- *"show cluster info" on page 967*
  - `show cluster info connection <parameters>]`

To show information about regular traffic:

- *"asg_ifconfig" on page 757*
- *"asg_conns" on page 725*
- *"asg_tracert" on page 851*

To show information about multicast traffic:

- *"asg_pim" on page 806*
- *"asg_igmp" on page 766*
- *"asg_mroute" on page 801*

To capture traffic:

- *"tcpdump" on page 992*

Monitoring Interfaces

To monitor the interfaces in your Security Group, use these commands:

- *"insights" on page 903*
- *"show cluster info" on page 967*
  - `show cluster info interfaces`
- *"asg_ifconfig" on page 757*
- `show interfaces` (in Gaia gClish)

Monitoring VPN Tunnels

Because VPN tunnels synchronize between all Security Group Members, you need to use traditional tools to monitor VPN 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.
- In the Traditional VSX mode, search for the "**SNMP Monitoring**" section in the *R82 VSX Administration Guide* for VSX-related SNMP information.

CLI Tools

Notes:

- In the VSNext mode / Traditional VSX mode, you must run these commands in the context of the applicable Virtual Gateway / Legacy Virtual System.
- For more information about these commands, see the *R82 CLI Reference Guide*.

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
  ```

Hardware Monitoring on Security Groups

To monitoring the hardware components in your Security Group, use these commands:

- *"insights" on page 903*
- *"asg stat" on page 829*
- *"asg monitor (on Security Groups)" on page 792*
- *"show cluster info" on page 967*
  - `show cluster info overview [live] [format json]`
  - `show cluster info cpu [live] [format json]`
  - `show cluster info interfaces [live] [format json]`

Troubleshooting on Security Groups

This section provides troubleshooting commands on Security Groups.

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.

  This command runs the Check Point Support Data Collector (CPSDC) tool that is described in sk164414.

- HealthCheck Point (HCP) - see *"hcp" on page 899*.

In addition, see:

- *"CPView" on page 641*
- *"insights" on page 903*

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	■ For information about the Firewall drops, run this command in the Expert mode:
		`g_fw ctl zdebug + drop`
		■ For information about the Software Blade Updates, run this command in the Expert mode:
		`asg_swb_update_verifier`
		See *"asg_swb_update_verifier" on page 843*.
		■ Examine the Security Gateway logs on the Management Server or Log Server

5	Session	■ For information about the Connections table, run this command in the Expert mode:
		`g_fw tab -t connections -s`
		■ For information about the Firewall drops, run this command in the Expert mode:
		`g_fw ctl zdebug + drop`
		■ For information about the performance, run these commands in Gaia gClish:
		`insights`
		`show cluster info`
		See:
		• *"insights" on page 903*.
		• *"show cluster info" on page 967*.

4	Transport	■ For information about the Correction Layer and traffic flow, use the `g_tcpdump` command in the Expert mode See *"tcpdump" on page 992*. ■ For information about the VPN, examine the Security Gateway logs on the Management Server or Log Server

Layer Number	Layer Name	Recommended Diagnostic Commands

3	Network	■ In the Expert mode, run these commands:
		• For information about the traffic:
		`asg_ifconfig`
		See *"asg_ifconfig" on page 757*.
		• For information about the routes:
		`asg_route`
		See *"asg_route" on page 813*.
		• For information about the dynamic routes:
		`asg_dr_verifier`
		See *"asg_dr_verifier" on page 732*.
		• For information about the routes:
		`netstat -rn`
		• For information about the routes:
		`route`
		■ In Gaia gClish, run these commands:
		• For information about the traffic:
		`asg_ifconfig`
		See *"asg_ifconfig" on page 757*.
		• For information about the routes:
		`asg_route`
		See *"asg_route" on page 813*.
		• For information about the routes:
		`show route ...`

2	Data Link	■ For information about the Bridge interfaces, run this command in Gaia gClish or the Expert mode: `asg_br_verifier` See *"asg_br_verifier, asg_brs_verifier" on page 720*.

Layer Number	Layer Name	Recommended Diagnostic Commands

1	Physical	■ Run this command in Gaia gClish:
		`show maestro port <Port>`
		■ For information about the Bond interfaces, run this command in the Expert mode:
		`cat /proc/net/bonding/<Name of Bond Interface>`
		■ For information about the Port Link, run this command in the Expert mode:
		`ethtool ethsBP<X>-<XX>`
		■ For information about the interface statistics, run this command in the Expert mode:
		`ethtool -S ethsBP<X>-<XX>`

Working with Command Line

This chapter shows the list of commands for Scalable Platforms:

- ElasticXL Cluster
- Security Group (in Maestro and on Scalable Chassis)
- Maestro Orchestrator

Syntax Legend for CLI Commands

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.

Character	Description
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

Command Completion in Gaia gClish

Important - On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

You can automatically complete a command.

This saves time, and can help if you are not sure what to type next.

Press these keys...	To do this ...

<TAB>	Complete or fetch the keyword.
	Example:
	`HostName> set in<TAB>`
	`inactivity-timeout - Set inactivity timeout`
	`interface - Displays the interface related parameters`
	`HostName> set in`

<SPACE><TAB>	Show the arguments that the command for that feature accepts.
	Example:
	`HostName> set interface<SPACE><TAB>`
	`eth0 eth1 lo`
	`HostName> set interface`

<ESC><ESC>	See possible command completions.
	Example:
	`HostName> set inter<ESC><ESC>`
	`set interface VALUE ipv4-address VALUE mask-length VALUE`
	`set interface VALUE ipv4-address VALUE subnet-mask VALUE`
	`set interface VALUE ipv6-address VALUE mask-length VALUE`
	`set interface VALUE {comments VALUE mac-addr VALUE mtu VALUE state VALUE speed VALUE duplex VALUE auto-negotiation VALUE}`
	`set interface VALUE {ipv6-autoconfig VALUE}`
	`HostName> set inter`

Press these keys...	To do this ...

SHIFT ?	Get help on a feature or keyword.
	Example:
	`HostName> set interface<SPACE><SHIFT ?>`
	`interface: specifies the interface name`
	`This operation configures an existing interface`
	`HostName>`

UP arrow DOWN arrow	Browse the command history.
LEFT arrow RIGHT arrow	Move the cursor inside the current command to edit it.
Enter	Run the current command. The cursor does not have to be at the end of the line.

Command History in Gaia gClish

Important - On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

You can recall commands you have used before, even in previous sessions.

Command	Description
?	Recall the previous command.
`history`	Show the last 100 executed commands.
`!!`	Run the last executed command.
`!nn`	Run a specific previous command from the history list. Example: `!14`
`!-nn`	Run the `nn`th previous command from the history list - counting from the most recent command. For example, entering `!-3` runs the third from the last command from the history list.
`!str`	Run the most recent command that starts with `str`. Example: `!show`

Command Reuse

You can combine word designators with history commands to refer to specific words used in previous commands.

Words are numbered from the beginning of the line with the first word being denoted by `0` (digit zero).

Use a colon (`:`) to separate a history command from a word designator.

For example, you could enter `!!:1` to refer to the first argument in the previous command.

In the command "`show interfaces`", the `interfaces` is word 1.

Word Designator	Meaning
`0`	The operation word.
`n`	The `n`th word.
`^`	The first argument (that is, word 1).

Word Designator	Meaning
`$`	The last argument.
`%`	The word matched by the most recent `\?str\?` search.

Immediately after word designators, you can add a sequence of one or more of these modifiers, each preceded by a colon:

Modifier	Meaning
`p`	Print the new command, but do not execute.
`s/str1/str2`	Replace `str1` with `str2` in the first occurrence of the word, to which you refer.
`g`	Apply changes over the entire command. Use this modified in conjunction with `s`, as in `gs/str1/str2`.

Moving and Editing in Gaia gClish

Important - On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

This table shows the keyboard keys you can use to move within the syntax and edit the syntax:

Keys	Action
CTRL L	Clears the screen and shows the current typed command at the top of the screen.
Home, **CTRL A**	Moves to the beginning of the command line.
End, **CTRL E**	Moves to the end of the command line.
Left-Arrow, **CTRL B**	Moves to the previous character to the left of the cursor.
Right-Arrow, **CTRL F**	Moves to the next character to the right of the cursor.
CTRL Right-Arrow, **ALT F**	Jumps to the next word to the right of the cursor.
Backspace, **CTRL H**	Deletes the character to the left of the cursor.
ALT D	Deletes the word to the right of the cursor (if the cursor is located at the word start).
CTRL ALT H	Deletes the word to the left of the cursor (if the cursor is located at the word end).
CTRL U	Deletes the current syntax completely.
CTRL N	Shows the commands in the history list - from the current position down the list (to the most recent command). Each time you press these keys, it shows another previous command down the list.

Keys	Action
CTRL P	Shows the commands in the history list - from the current position up the list (to the oldest command). Each time you press these keys, it shows another previous command up the list.
CTRL R	Searches in the history list for the string you enter and shows the matching command.

Configuration Lock in Gaia gClish

Important - On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

Only one user can have Read/Write access to Gaia configuration database at a time. All other users can log in with Read-Only access to see configuration settings, as specified by their assigned roles in Gaia OS.

When you log in and no other user has Read/Write access, you get an exclusive configuration lock with Read/Write access. If a different user already has the configuration lock, you have the option to override their lock.

If you:

- Override the lock, then the other user stays logged in with Read-Only access.
- Do not override the lock, then you cannot modify the settings.

The "lock database" and "lock database" commands

Description

Use the "`lock database override`" and "`unlock database`" commands to get exclusive read-write access to the Gaia database by taking write privileges away from other administrators logged into the system.

Syntax

```
lock database override
unlock database
```

Comments

- Use these commands with caution.

  The administrator, whose write access is revoked, does not receive a notification.
- The "`lock database override`" command is identical to the "`set config-lock on override`" command.
- The "`unlock database`" command is identical to the "`set config-lock off`" command.

The "config-lock" commands

Description

Configures and shows the state of the configuration lock on Gaia configuration database.

Syntax

```
set config-lock
      off
      on [timeout <5-900>] override
```

```
show
      config-lock
      config-state
```

Parameters

Parameter	Description
`off`	Turns off the configuration lock.
`on`	Turns on the configuration lock. The default timeout value is 300 seconds.
`timeout <5-900>`	Optional parameter. Turns on the configuration lock for the specified interval in seconds.

Comments

- The "`set config-lock on override`" command is identical to the "`lock database override`" command.
- The "`set config-lock off`" command is identical to the "`unlock database`" command.

Summary of Gaia gClish Commands

Important - On Scalable Platforms, you must run the applicable commands in Gaia gClish of the applicable Security Group.

This section shows the list of commands available in Gaia gClish.

To show the list of all available Gaia gClish commands:

Step	Instructions
1	Connect to the command line on your Security Group.
2	Log in to Gaia gClish.
3	Press the <TAB> key on the keyboard.

To show the list of available Gaia gClish '`show`' commands:

Step	Instructions
1	Connect to the command line on your Security Group.
2	Log in to Gaia gClish.
3	Type: `show`
4	Press the <SPACE> key and then the <TAB> key on the keyboard.

To show the list of available Gaia gClish '`add`' commands:

Step	Instructions
1	Connect to the command line on your Security Group.
2	Log in to Gaia gClish.
3	Type: `add`
4	Press the <SPACE> key and then the <TAB> key on the keyboard.

To show the list of available Gaia gClish '`set`' commands:

Step	Instructions
1	Connect to the command line on your Security Group.
2	Log in to Gaia gClish.
3	Type: `set`
4	Press the <SPACE> key and then the <TAB> key on the keyboard.

To show the list of available Gaia gClish '`delete`' commands:

Step	Instructions
1	Connect to the command line on your Security Group.
2	Log in to Gaia gClish.
3	Type: `delete`
4	Press the <SPACE> key and then the <TAB> key on the keyboard.

Common CLI Commands

asg alert

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Best Practices:

- Configure SNMP Trap OIDs in Gaia gClish as described in *"SNMP for Security Groups" on page 647*.
- Run the "`insights`" command (*"insights" on page 903*) or the "`hcp`" command (*"hcp" on page 899*) on a regular basis.

Description

The "`asg alert`" command is an interactive wizard that configures system 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.

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 "`insights`" command or the "`hcp`" command to confirm the issue is resolved.

The "`asg alert`" wizard has these options:

Option	Description
1) Full Configuration Wizard	Creates a new alert.
2) Edit Configuration	Changes an existing alert.
3) Show Configuration	Shows existing alert configuration.
4) Run Test	Runs a test simulation to make sure that the alert works correctly.

Alert Configuration Procedure

Procedure

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in.
3	Run: `asg alert`
4	Enter the number of the applicable option and press Enter: ■ **1** for **Full Configuration Wizard**. ■ **2** for **Edit Configuration**.
5	Enter the number of the applicable option and press Enter: ■ **1** for **SMS** (see the menu below). ■ **2** for **Email** (see the menu below). ■ **3** for **Log** (see the menu below).
6	Configure the required parameters as prompted by the wizard.

SMS Alert Parameters

Explanation

Parameter	Description
SMS provider URL	Fully qualified URL to your SMS provider.
HTTP proxy and port	Optional. Configure only if the Security Gateway requires a proxy server to reach the SMS provider.
SMS rate limit	Maximum number of SMS messages sent per hour. If there are too many messages, they can be combined together.
SMS user text	Custom prefix for SMS messages.

Email Alert Parameters

Explanation

Parameter	Description
SMTP server IP	One or more SMTP servers to which the email alerts are sent.
Email recipient addresses	One or more recipient email address for each SMTP server.
Periodic connectivity checks	Tests run periodically to confirm connectivity with the SNMP servers. If there is no connectivity, alert messages are saved and sent in one email when connectivity is restored.
Interval	Interval, in minutes, between connectivity tests.
Sender email address	Email address of the sender for alerts.
Subject	Subject header text for the email alert.
Body text	User defined text for the alert message.

Log Alert Event Types

Explanation

There are no parameters to configure.

1. Select event types for which to send alerts:
   - All event types (enter: `all`).
   - None of the event types (enter: `none`).
   - Specific event types (enter the required numbers).

     Some Hardware Monitor event types apply only to Scalable Chassis.
2. Configure the **Log Mode** to one of these:
   - **Enabled** (enter: `e`).

     The Security Group sends an alert for the selected events.
   - **Disabled** (enter: `d`).

     The Security Group does not send alerts for the selected events.
   - **Monitor** (enter: `m`).

     The Security Group generates a log entry instead of an alert.

System Event Types

```
################################################
#  Welcome to the Log Full Configuration Wizard  #
################################################

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 none or 1,4 or 1,3-7,10)
>
```

asg_arp

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Shows the ARP cache table.

Syntax

```
asg_arp -h
```

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

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows the ARP cache table.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-i <Name of Interface>`	Shows the ARP entries only for the specified interface.
`--legacy`	Shows the ARP entries in the legacy format.
`-m <MAC Address>`	Shows the ARP entries only for the specified MAC Address.
`<Hostname>`	Shows the ARP entries only for the specified Hostname.
`-v`	Shows the ARP entries in the verbose format (also shows the IDs of the Security Group Members).
`--verify`	Runs MAC Address verification on Security Group Members.

Examples

Example 1 - Default Output

This example shows the ARP cash in the Default Mode:

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example 2 - Verbose Output

This example shows the ARP cash in the Verbose Mode:

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example 3 - Output for Verifying MAC Addresses

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

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example 4 - 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@SG-s01-01:0]# 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] SG-s01-01> fw ctl get int fwha_mac_magic
-*- 4 sgms: 1_01 1_02 2_02 2_03 -*-
fwha_mac_magic = 22
[Global] SG-s01-01>
```

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

Example:

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example 5 - Legacy Output

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

```
[Expert@SG-s01-01:0]# 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                      ether   00:1C:7F:02:04:FE   C                     Sync
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@SG-s01-01:0]#
```

asg_blade_config

Warning - This command is intended for advanced troubleshooting.
Do not run this command, unless Check Point Support explicitly asked you to do so.

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Shows advanced information about the Security Group configuration.

Configures advanced settings in the Security Group:

- Copies the Security Group Member configuration from the local Security Group Member to other Security Group Members in the Security Group
- Changes the synchronization start IP address
- Resets the system uptime value
- Fetches the policy from the Management Server

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.

Syntax

```
asg_blade_config
      dynamic_port_allocation {on | off | stat}
      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_max_members_for_port_range <Max Members> [<Max Sites>]
      set_sync_start_ip <Start IP Address>
      show_sp_failover
      stop_auto_reboot {on | off}
      upgrade_cu
      upgrade_start <New Version> [cu]
      upgrade_stat
      upgrade_stop
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help.
`dynamic_port_allocation {on | off | stat}`	Configures the dynamic local port allocation: ■ `on` - Enables ■ `off` - Disables ■ `stat` - Shows the current status
`fetch_smc`	Fetches the security policy from the Management Server and distributes it to all Security Group Members.
`full_sync <IP Address>`	Performs the Full Sync from the specified Security Group Member.
`get_smo_ip`	Shows the SMO IP Address from the Cluster Control Protocol (CCP) packets within the Security Group.
`is_in_pull_conf_group`	Shows whether the Security Group Member is part of the Pulling Configuration Group.

Parameter	Description
`is_in_security_group`	Shows whether the Security Group Member is part of the Security Group.
`pull_config`	Pulls the configuration from other Security Group Members.
`reset_sic -reboot_all <Activation Key>`	Starts a SIC cleanup (resets the SIC).
`set_max_members_for_port_range <Max Members> [<Max Sites>]`	Configures the port range and ports for each Security Group Member.
`set_sync_start_ip <Start IP Address>`	Configures the internal Sync network. **Warning** - ElasticXL does not support this command.
`show_sp_failover`	Shows the Security Group failover logs.
`stop_auto_reboot {on | off}`	Configures the automatic reboots: ■ `on` - Enables the automatic reboots ■ `off` - Disables the automatic reboots
`upgrade_cu`	Deprecated. Enables the Connectivity Upgrade mode (runs an iteration).
`upgrade_start <New Version> [cu]`	Deprecated. Start the upgrade procedure from the current version to the specific version. The option "`cu`" enables the Connectivity Upgrade mode.
`upgrade_stat`	Deprecated. Shows the Connectivity Upgrade progress.
`upgrade_stop`	Deprecated. Stops the Connectivity Upgrade.

asg_blade_stats

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows statistics for internal packet forwarding in the Correction Layer.

Syntax

```
asg_blade_stats
      all
      arp_forw
      corr
      iterator
      vpn
      -c {a | d | f | i | v}
```

Parameters

Parameter	Description
`all`	Shows all statistics for the Correction Layer.
`arp_forw`	Shows the ARP forwarding statistics.
`corr`	Shows the aggregated statistics for the Correction Layer.
`iterator`	Shows the last iterator statistics.
`vpn`	Shows the VPN forwarding statistics.
`-c {a | d | f | i | v}`	Shows the ICMP forwarding statistics.

Examples

Example 1 - "asg_blade_stats corr"

```
[Expert@SG-s01-01:0]# asg_blade_stats corr
1_01:

Getting stats for SXL device 0, may take a few seconds...

Cluster Correction Stats (All Traffic):
-------------------------------------------------------
Sent packets:                   319067 (0 with metadata)
Sent bytes:                     26,801,628
Received packets:               1068 (0 with metadata)
Received bytes:                 89,712
Send errors:                    0
Receive errors:                 0
Local asymmetric conns:         28299
ICMP ERROR forwarded packets:           0
ICMP ERROR forwarded bytes:             0
VS Stateless forwarded packets:         0
VS Stateless forwarded bytes:           0
-------------------------------------------------------------------
1_02:

Getting stats for SXL device 0, may take a few seconds...

Cluster Correction Stats (All Traffic):
-------------------------------------------------------
Sent packets:                   1974 (0 with metadata)
Sent bytes:                     165,816
Received packets:               159509 (0 with metadata)
Received bytes:                 13,398,756
Send errors:                    0
Receive errors:                 0
Local asymmetric conns:         79743
ICMP ERROR forwarded packets:           0
ICMP ERROR forwarded bytes:             0
VS Stateless forwarded packets:         0
VS Stateless forwarded bytes:           0
-------------------------------------------------------------------
1_03:

Getting stats for SXL device 0, may take a few seconds...

Cluster Correction Stats (All Traffic):
-------------------------------------------------------
Sent packets:                   0 (0 with metadata)
Sent bytes:                     0
Received packets:               160464 (0 with metadata)
```

```
Received bytes:                 13,478,976
Send errors:                    0
Receive errors:                 0
Local asymmetric conns:         107948
ICMP ERROR forwarded packets:           0
ICMP ERROR forwarded bytes:             0
VS Stateless forwarded packets:         0
VS Stateless forwarded bytes:           0
------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

Example 2 - "asg_blade_stats iterator"

```
[Expert@SG-s01-01:0]# asg_blade_stats iterator
1_01:

Last Iterator Statistics:
-------------------------------------------------------------
Start time:                              Tue Oct 15 09:19:10 2024
Running time:                            3 Seconds
Status:                                  finished
Reason:
Total connections iterated:              205
Connections w/ sync action:              0
-------------------------------------------------------------
1_02:

Last Iterator Statistics:
-------------------------------------------------------------
Start time:                              Tue Oct 15 09:19:04 2024
Running time:                            4 Seconds
Status:                                  finished
Reason:
Total connections iterated:              455
Connections w/ sync action:              0
-------------------------------------------------------------
1_03:

Last Iterator Statistics:
-------------------------------------------------------------
Start time:                              Tue Oct 15 09:19:10 2024
Running time:                            4 Seconds
Status:                                  finished
Reason:
Total connections iterated:              325
Connections w/ sync action:              0
-------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

Example 3 - "asg_blade_stats arp_forw"

```
[Expert@SG-s01-01:0]# asg_blade_stats arp_forw
1_01:

ARP Forwarding Statistics:
-------------------------------------------------------------
arp replies:                                                4
forwarded arp replies (pseudo interfaces):                  0
-------------------------------------------------------------
1_02:

ARP Forwarding Statistics:
-------------------------------------------------------------
arp replies:                                             2723
forwarded arp replies (pseudo interfaces):                  0
-------------------------------------------------------------
1_03:

ARP Forwarding Statistics:
-------------------------------------------------------------
arp replies:                                                0
forwarded arp replies (pseudo interfaces):                  0
-------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

Example 4 - "asg_blade_stats vpn"

```
[Expert@SG-s01-01:0]# asg_blade_stats vpn
1_01:

VPN Forwarding Statistics:
-------------------------------------------------------------
encrypted forwarded packets:            0
-------------------------------------------------------------
1_02:

VPN Forwarding Statistics:
-------------------------------------------------------------
encrypted forwarded packets:            0
-------------------------------------------------------------
1_03:

VPN Forwarding Statistics:
-------------------------------------------------------------
encrypted forwarded packets:            0
-------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

asg_br_verifier, asg_brs_verifier

This command is supported only on these:

- Maestro Security Group in the Traditional VSX mode
- Scalable Chassis Security Group in the Traditional VSX mode

Notes:

- You can run the "`asg_br_verifier`" command in Gaia gClish or in the Expert mode.
- You must run the "`asg_brs_verifier`" command in the Expert mode.
- You must run the "`asg_br_verifier`" command in the context of the specific Virtual System in the Bridge Mode.
- You can run the "`asg_brs_verifier`" command in the context of any Virtual System to get the output for all Virtual Systems in the Bridge Mode.
- These two commands also confirm that the "`fdb_shadow`" tables are the same for the Virtual System on different Security Group Members.

Description

Confirms that there are no bridge configuration problems in 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).
`-v`	Shows verbose formatted output. The "`-v`" and "`-d`" options are mutually exclusive.

Examples

Example 1 - Output in a normal state

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example 2 - Output in a state of wrong configuration

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

asg_clear_table

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Deletes connections from the "Connections" kernel table on the Security Group Members.

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

Warning - If you are connected to the Security Group over SSH, your connection is disconnected.
Run this command only over a console connection, or from a Maestro Orchestrator.

Syntax

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

Parameters

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

Examples

```
[Expert@SG-s01-01:0]# asg_clear_table
You are about to perform connections table entry deletion on
members: 1_01,2_01
This action may terminate your current connection

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

Connections table entry deletion requires auditing
Enter your full name: admin
Enter reason for connections table entry deletion [Maintenance]:
lab test
WARNING: Connections table entry deletion on members: 1_01,2_01,
User: admin, Reason: lab test
```

asg_conns

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows the summary information for the "Connections" kernel table.

Related Commands

- *"insights" on page 903*
- In Gaia gClish, run "`show cluster info connection <parameters>`" (*"show cluster info" on page 967*)

Syntax

```
asg_conns
        -h
        -6
```

Parameters

Parameter	Description
No Parameters	Shows the information only for IPv4.
`-h`	Shows the built-in help.
`-6`	Shows the information only for IPv6.

Examples

```
[Expert@SG-s01-01:0]# 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
[Expert@SG-s01-01:0]#
```

asg_cores_stats

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows this information:

- Number of physical CPU cores on Security Group Members
- Number of IPv4 CoreXL Firewall instances on Security Group Members
- Number of IPv6 CoreXL Firewall instances on Security Group Members
- Number of IPv4 CoreXL SND instances (PPAK) on Security Group Members
- Number of IPv6 CoreXL SND instances (PPAK) on Security Group Members
- Affinity of interfaces to CPU cores on Security Group Members

Syntax

```
asg_cores_stats
```

Related Commands

- In Gaia gClish:
  - `fw ctl multik stat`
  - `fw6 ctl multik stat`
  - `fw ctl affinity <flags>`
  - `fw6 ctl affinity <flags>`
- In the Expert mode:
  - `g_fw ctl multik stat`
  - `g_fw6 ctl multik stat`
  - `g_fw ctl affinity <flags>`
  - `g_fw6 ctl affinity <flags>`

Examples

This output is from a Maestro Security Group with 2 x 6800 and 1 x 7000 Security Appliances.

```
[Expert@SG-s01-01:0]# asg_cores_stats
Number of physical cores on all Members is:
-------------------------------------
-*- 2 blades: 1_01 1_03 -*-
20
-*- 1 blade: 1_02 -*-
32

Number of IPv4 corexl instances on all Members is:
-----------------------------------------
-*- 3 blades: 1_01 1_02 1_03 -*-
18

Number of ppak cores on all Members is:
---------------------------------
-*- 2 blades: 1_01 1_03 -*-
2
-*- 1 blade: 1_02 -*-
14

Ppak core affinity on all Members is:
-----------------------------------
-*- 1 blade: 1_01 -*-
ethsBP1-01-TxRx-0: 00001
ethsBP1-02-TxRx-0: 00001
... ... (truncated) ... ...
ethsBP1-03-TxRx-15: 20000
ethsBP1-04-TxRx-15: 20000
-*- 1 blade: 1_02 -*-
ethsBP1-01-TxRx-0: 00000001
ethsBP1-02-TxRx-0: 00000001
... ... (truncated) ... ...
ethsBP1-03-TxRx-29: 40000000
ethsBP1-04-TxRx-29: 40000000
-*- 1 blade: 1_03 -*-
ethsBP1-01-TxRx-0: 00001
ethsBP1-02-TxRx-0: 00001
... ... (truncated) ... ...
ethsBP1-03-TxRx-15: 20000
ethsBP1-04-TxRx-15: 20000
[Expert@SG-s01-01:0]#
```

asg_cp2blades

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

When you connect to a Security Group, you work on one of the Security Group Members.

All Check Point configuration files must be identical on all Security Group Members.

Meaning, if you created or edited a Check Point configuration file, then you must copy to all other Security Group Members.

This command makes this task easier.

Note - You can use this command to copy any file from the current Security Group Member to other Security Group Members.

Syntax

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

Parameters

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-r`	Copy folders and directories that contain files.
`-s`	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: `*.bak.<date>.<time>`
`<Source Path>`	Full path and name of the file to copy.
`<Destination Path>`	Full path of the destination. If not specified, the command copies the file to the relative source file location.

Examples

```
[Expert@SG-s01-01:0]# asg_cp2blades /home/admin/note.txt
Operation completed successfully
[Expert@SG-s01-01:0]#
[Expert@SG-s01-01:0]# cat /home/admin/note.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
hello world
[Expert@SG-s01-01:0]#
```

asg_dr_verifier

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Verifies the consistency of the dynamic routing configuration (OSPF, BGP, and RIP) between the Security Group Members.

Syntax

```
asg_dr_verifier
      -a
      {-6 | --ipv6}
      -b <SGM IDs>
      --filter {all | bgp | ospf | rip}
      --vs <VS ID>
```

Parameters

Parameter	Description
No Parameters	Verifies the configuration for all dynamic routes (OSPF, BGP, and RIP), for IPv4 and IPv6.
`-6` `--ipv6`	Verifies the configuration for all dynamic routes (OSPF, BGP, and RIP), only for IPv6.
`-a`	Includes the Security Group Members that are in the "DOWN" state.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`--filter {all | bgp | ospf | rip}`	Verifies the configuration for the specified dynamic routing protocol: ■ `all` - For all dynamic routing protocols (OSPF, BGP, and RIP) - this is the default ■ `bgp` - Only for BGP ■ `ospf` - Only for OSPF ■ `rip` - Only for RIP
`--vs <VS ID>`	Specifies the IDs of the Traditional VSX Virtual Systems. Applies to the Traditional Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.

Parameter	Description
`--vs <VS ID>`	Specifies the IDs of the Traditional VSX Virtual Systems. Applies to the Traditional Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.

asg_dst_route

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Shows statistics about the OS route cache.

Configures settings for the OS route cache.

Related Commands

- *"asg_route" on page 813*
- *"asg_mroute" on page 801*

Syntax

```
asg_dst_route
      -h
      -b <SGM IDs>
      -d
      -e
      -g {increase | decrease}
      -s
      -v
```

Parameters

Parameter	Description
-h --help	Shows the built-in help.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-d` `--disable`	Disables the destination-based routing.
`-e` `--enable`	Enables the destination-based routing.
`-g {increase | decrease}`	Increase or decreases the aggressiveness for the route cache garbage collection.
`-s` `--stats`	Shows the statistics.
`-v` `--verify`	Verifies the configuration consistency (this is the default operation).

Examples

Example 1 - Standard output

```
[Expert@SG-s01-01:0]# asg_dst_route
+-------------------------------------------------------------------
---------------+
| SGM         | Current Status             | Persistency
              |
+-------------------------------------------------------------------
---------------+
| 1_01        | Error                      | Source+Dest based
route             |
| 2_01        | Error                      | Source+Dest based
route             |
+-------------------------------------------------------------------
---------------+
[Expert@SG-s01-01:0]#
```

Example 2 - Statistics

```
[Expert@SG-s01-01:0]# asg_dst_route -s
+-----------------------------------------------+
| SGM  | Cache load | Hit rate   | Effectiveness |
+-----------------------------------------------+
| 2_01 | -22700 %   | 0 %        | 100 %         |
+-----------------------------------------------+
[Expert@SG-s01-01:0]#
```

asg_dxl

Warning - Do not use this command to change the configuration, unless Check Point Support explicitly asked you to do so.

Best Practice - Follow the instructions in *"Working with the Distribution Mode" on page 554*.

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows and configures the distribution mode (DXL) options.

The distribution mode are (for more information, see *"Working with the Distribution Mode" on page 554*.):

Mode Number	Mode Name	Packet Assignment to a Security Group Member
0	General	The ElasticXL Cluster / Maestro Orchestrators / Scalable Chassis SSMs assign packets to a Security Group Member based only on the packet's Source IP address and the Destination IP address. If Layer 4 distribution is enabled, the ElasticXL Cluster / Maestro Orchestrators / SSMs assign packets to a Security Group Member based on the packet's Source IP address, Source Port, Destination IP address, and Destination Port. On Scalable Chassis, this mode applies to all SSMs in the Scalable Chassis.
1	User (Internal)	Packets are assigned to a Security Group Member based only on the packet's Destination IP address. If Layer 4 distribution is enabled, the ElasticXL Cluster / Maestro Orchestrator / Scalable Chassis SSM assigns packets to a Security Group Member based on the packet's Source Port and the Destination IP address. On Scalable Chassis, this mode applies to one SSM. **Note** - Scalable Platforms do not support Hide NAT when the Distribution Mode "User (Internal)" is configured on one of more outbound interfaces (Known Limitation SPC-1682).
2	Network (External)	Packets are assigned to a Security Group Member based only on the packet's Source IP address. If Layer 4 distribution is enabled, the ElasticXL Cluster / Maestro Orchestrator / Scalable Chassis SSM assigns packets to a Security Group Member based on the packet's Source IP address and Destination Port. On Scalable Chassis, this mode applies to one SSM. **Note** - Scalable Platforms do not support Hide NAT when the Distribution Mode "Network (External)" is configured on one or more inbound interfaces (Known Limitation SPC-1682).

Syntax

Run the "`asg_dxl`" command or the "`asg dxl`" command.

```
asg_dxl
      help [-v]
      bmac
      calc <Source IP Address> <Destination IP Address>
<Distribution Mode or Name of Interface>
      dist [<Name of File>] [-j]
      export <Name of File>
      general_mode
      import <Name of File>
      init
      l4_mode
      load_analyzer
            -f <Name of CSV File>
            [-b <1-12>]
            [-d {0 | 1 | 2}]
            [-m <16-32>]
            [-s {0 | 1}]
            [-t <Test Mask>]
            [-6 {0 | 1}]
            [-v]
      md5sum
      query <Source IP Address> <Source Port> <Destination IP
Address> <Destination Port> <Protocol>
      size
      stat [-v]
      static
            get <Name of File>
            set <Name of File>
            stop
      update
      verify [SSM ID]
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help.
`help`	Shows the built-in help.
`help -v`	Shows the verbose built-in help (shows more sub-commands).

Parameter	Description
`bmac`	■ On ElasticXL Cluster and Maestro: Shows the Base MAC Address for each Site. ■ On Scalable Chassis: Shows the Base MAC Address for each SSM.
`calc <Parameters>`	Calculates the DXL decision based on these parameters: ■ Source IP Address ■ Destination IP Address ■ Distribution Mode, or Name of Interface The Distribution Mode is one of these values: • `0` - "General" mode. • `1` - "User" mode. • `2` - "Network" mode.
`dist [<Name of File>] [-j]`	Show or configures the distribution mode. The parameter "`-j`" specify to use the JSON format.
`export <Name of File>`	Exports the DXL configuration to the specified file.
`general_mode`	Shows the status of the DXL "General" mode (enabled or disabled).
`import <Name of File>`	Imports the DXL configuration from the specified file.
`init`	Initializes the DXL configuration.
`l4_mode`	Shows the status of the DXL "Layer 4" mode (enabled or disabled).

Parameter	Description

`load_analyzer <Parameters>`	Analyzes the load of the Security Group.
	■ `-f <Name of CSV File>`
	Specifies the path and the name of the CSV file that contains records in this format:
	`<Source IP Address>,<Destination IP Address>, [{internal | external}],<Percent of Load>`
	Example:
	`69.78.32.247,173.209.194.151,internal,6.89%`
	■ `-b <1-12>`
	Specifies the number of Security Group Members, on which to run the command.
	Default: The current number of Security Group Members.
	■ `-d {0 | 1 | 2}`
	Specifies the Distribution Mode, for which to run the command:
	• `0` - "General" mode.
	• `1` - "User-Network" mode.
	• `2` - "Per-Port" mode.
	Default: The current Distribution Mode.
	■ `-m <16-32>`
	Specifies the Mask Range, the number of bits to calculate the optimal mask.
	Default: 16.
	■ `-s {0 | 1}`
	Specifies whether the VPN SPI mode is enabled for this command:
	• `0` - VPN SPI mode is disabled.
	• `1` - VPN SPI mode is enabled.
	Default: The current VPN SPI mode.
	■ `-t <Test Bit Mask>`
	Specifies the Distribution Bit Mask, for which to run the command.
	■ `-6 {0 | 1}`
	Specifies whether the IPv6 mode is enabled for this command:
	• `0` - IPv6 mode is disabled.
	• `1` - IPv6 mode is enabled.
	Default: The current IPv6 mode.
	■ `-v`
	Specifies the verbose output.

`md5sum`	Calculate the MD5 sum of the DXL configuration.

Parameter	Description
`query <Parameters>`	Shows the DXL decision for the specified 5-tuple that currently exists in the "Connections" kernel table.
`size`	Shows the size of the DXL table.
`stat [-v]`	Shows the DXL status - summarized or verbose.
`static <Parameters>`	Controls the manual assignment of the distribution list: ■ `get <Name of File>` Shows the current distribution list from the specified file.. ■ `set <Name of File>` Configures the distribution based on the specified file. ■ `stop` Returns to the dynamic distribution method.
`update`	Forces the DXL update.
`verify [<SSM ID>]`	Applies only to Scalable Chassis. Compare the configuration signatures between the SSMs and the DXL distribution.

asg_excp_conf

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

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 outgoing connections that the Security Group initiates.
- In VSNext / Traditional VSX mode, you must run this command in the context of the applicable Virtual Gateway / Legacy Virtual System.
- This command supports a maximum of 15 exceptions
  (in the Traditional 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> <Source IP Address> <Source Port> <Destination IP
Address> <Destination Port>
```

Parameters

Parameter	Description
No Parameters	Shows the built-in help.

Parameter	Description
`clear`	Deletes all exception entries.
`del <ID>`	Deletes the specified exception entry. Use the "`get`" parameter to see the IDs. ID numbers start from 0 (zero).
`get`	Shows all exception entries and their IDs.

Parameter	Description
`set <Parameters>`	Configures a new exception entry. **Notes:** ■ This command does **not** support wildcard characters (`*` or `?`) or the word "`any`". You must always configure the exact values of the connection 4-tuple. ■ The order of these arguments is predefined (for example, "*<src_ip>*" is always the second argument). The "*<Type>*" parameter 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 "*<Type>*" value. The exception type is one of these values: ■ `1` - Matches the inbound connection by the Source IP address ■ `2` - Matches the inbound connection by the Destination IP address ■ `3` - Matches the inbound connection by the Source port ■ `4` - Matches the inbound connection by the Destination port ■ `5` - Matches the inbound connection by the Source IP address + Destination IP address ■ `6` - Matches the inbound connection by the Source IP address + Source port ■ `7` - Matches the inbound connection by the Source IP address + Destination port ■ `8` - Matches the inbound connection by the Destination IP address + Source port ■ `9` - Matches the inbound connection by the Destination IP address + Destination port ■ `10` - Matches the inbound connection by the Source port + Destination port ■ `11` - Matches the inbound connection by the Source IP address + Destination IP address + Source port ■ `12` - Matches the inbound connection by the Source IP address + Destination IP address + Destination port ■ `13` - Matches the inbound connection by the Source IP address + Source port + Destination port ■ `14` - Matches the inbound connection by the destination IP address + Source port + Destination port ■ `15` - Matches the inbound connection by the Source IP address + Destination IP address + Source port + Destination port

Examples

Example 1 - 'asg_excp_conf set'

```
[Expert@SG-s01-01:0] asg_excp_conf set 2 192.168.20.30 40000
172.16.40.50 80
1_01:
Exception entry added successfuly.
1_02:
Exception entry added successfuly.
1_03:
Exception entry added successfuly.
1_04:
Exception entry added successfuly.
2_01:
Exception entry added successfuly.
2_02:
Exception entry added successfuly.
2_03:
Exception entry added successfuly.
2_04:
Exception entry added successfuly.
[Expert@SG-s01-01:0]
```

Example 2 - 'asg_excp_conf get'

```
[Expert@SG-s01-01:0] 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@SG-s01-01:0]
```

Example 3 - 'asg_excp_conf del'

```
[Expert@SG-s01-01:0]# asg_excp_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@SG-s01-01:0]
```

Example 4 - 'asg_excp_conf clear'

```
[Expert@SG-s01-01:0] asg_excp_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@SG-s01-01:0]
```

asg_gre

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Shows configuration for GRE interfaces.

Syntax

```
asg_gre
       -h
       load
       stat
       verify
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`load`	Copies the GRE configuration file to all Security Group Members and loads the GRE configuration.
`stat`	Shows the GRE configuration.
`verify`	Verifies the GRE configuration on all Security Group Members.

asg_hd_space

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group

Note - You must run this command in the Expert mode.

Description

Shows the hard disk space.

Syntax

```
asg_hd_space
```

Examples

```
[Expert@SG-s01-01:0]# asg_hd_space

Total disk space:
[1_01]Disk /dev/sda: 240.1 GB, 240057409536 bytes, 468862128
sectors
[1_01]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.
[1_02]Disk /dev/sda: 240.1 GB, 240057409536 bytes, 468862128
sectors
[1_02]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.
[1_03]Disk /dev/md0: 314 MB, 314507264 bytes, 614272 sectors
[1_03]Disk /dev/md1: 25.2 GB, 25232801792 bytes, 49282816 sectors
[1_03]Disk /dev/md2: 974.7 GB, 974654341120 bytes, 1903621760
sectors
[1_03]Disk /dev/sda: 1000.2 GB, 1000204886016 bytes, 1953525168
sectors
[1_03]Disk /dev/sdb: 1000.2 GB, 1000204886016 bytes, 1953525168
sectors
[1_03]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.
[1_03]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.
[2_01]Disk /dev/sda: 240.1 GB, 240057409536 bytes, 468862128
sectors
[2_01]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.
[2_02]Disk /dev/sda: 240.1 GB, 240057409536 bytes, 468862128
sectors
[2_02]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.
[2_03]Disk /dev/md0: 314 MB, 314507264 bytes, 614272 sectors
[2_03]Disk /dev/md1: 33.5 GB, 33520746496 bytes, 65470208 sectors
[2_03]Disk /dev/md2: 966.4 GB, 966366396416 bytes, 1887434368
sectors
[2_03]Disk /dev/sda: 1000.2 GB, 1000204886016 bytes, 1953525168
sectors
[2_03]Disk /dev/sdb: 1000.2 GB, 1000204886016 bytes, 1953525168
sectors
[2_03]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.
[2_03]WARNING: fdisk GPT support is currently new, and therefore
in an experimental phase. Use at your own discretion.

Remaining free space for snapshots:
[1_01]35.13G
[1_02]35.12G
```

```
[1_03]645.82G
[2_01]7.92G
[2_02]10.38G
[2_03]649.39G
[Expert@SG-s01-01:0]#
```

asg_ifconfig

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You can run this command in Gaia gClish or in the Expert mode.
- If you run this command in the context of a Traditional VSX Virtual System, you can only see the output that applies to that context.

Description

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
Native	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.
Analyze	Shows accumulated traffic information and traffic distribution between Security Group Members.
Banalyze	Shows accumulated traffic information and traffic distribution between interfaces.

Note - The parameters "`analyze`" and "`banalyze`" are mutually exclusive. You cannot specify them in the same command.

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]]
```

Note - To run this command continuously, use "`asg_ifconfig_m`" instead of "`asg_ifconfig`".

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: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`<Name of Interface>`	Specifies the name of the interface.
`analyze`	Shows accumulated traffic information and traffic distribution between the Security Group Members. Use the "`-a`", "`-v`", and "`-d <Delay>`" parameters to show traffic distribution between interfaces.

Parameter	Description

`banalyze`	Shows accumulated traffic information and traffic distribution between the interfaces.
	Use the "`-a`", "`-v`", and "`-d <Delay>`" parameters to show traffic distribution between interfaces.
	By default, the traffic distribution table is not sorted.
	You can use these parameters to sort the traffic distribution table:
	■ `-rb` - Sort the output by the number of received (RX) bytes
	■ `-rd` - Sort the output by the number of received (RX) dropped packets
	■ `-rp` - Sort the output by the number of received (RX) packets
	■ `-tb` - Sort the output by the number of transmitted (TX) bytes
	■ `-td` - Sort the output by the number of transmitted (TX) dropped packets
	■ `-tp` - Sort the output by the number of transmitted (TX) packets
	For example, if you sort with the "`-rb`" option, the higher values appear at the top of the "`RX bytes`" column:
	`SGM ID  RX packets  RX bytes  RX dropped`
	`1_03  70%`
	`1_02  20%`
	`1_01  10%`

`-d <Delay>`	Delay, in seconds, between data samples. Default: 5 seconds.
`-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 the Active Site 1.

By default, the output shows the average traffic volume per second.

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

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@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

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@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

asg_igmp

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows 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.

Related Commands

- *"asg_pim" on page 806*
- *"asg_mroute" on page 801*

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: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

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@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

Example 2 - Shows IGMP Information for a specified interface

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

asg_ips_failover_behavior

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Configures how the IPS Software Blade behaves during a cluster failover.

Syntax

```
asg_ips_failover_behavior {connectivity | security}
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`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

- In Gaia gClish:

```
fw ctl get int fwha_ips_reject_on_failover
```

- In the Expert mode:

```
g_allc 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

asg_license_verifier

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Verifies licenses on Security Group Members.

Syntax

```
asg_license_verifier
      -h
      -c {enable | disable}
      -d <Number of Days>
      -v
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Runs the verification and shows the verdict.
`-c {enable | disable}`	Enables or disables the license validation during the start of the Expert mode shell.
`-d <Number of Days>`	Configures the number of days, during which the license validation does not show license problems after the last confirmation.
`-v`	Runs the verification and shows the verbose output.

Examples

```
[Expert@SG-s01-01:0]# asg_license_verifier -v
INFO:    Non VSX system detected
VALID:   License for 'Firewall-1' [mandatory feature 'fm']
verified successfully
VALID:   License for 'VPN' [mandatory feature 'vpnstrong']
verified successfully
VALID:   License for 'Software Blades' [mandatory feature 'swb']
verified successfully
VALID:   License for 'Identity Awareness' [mandatory feature
'identity'] verified successfully
VALID:   License for 'Acceleration' [mandatory feature 'cpls']
verified successfully
VALID:   License for 'Acceleration' [mandatory feature 'cluster-
u'] verified successfully
VALID:   License for 'Acceleration' [mandatory feature 'mpu']
verified successfully
VALID:   License for 'Acceleration' [mandatory feature 'sxl_vpn']
verified successfully
VALID:   License for 'Acceleration' [mandatory feature 'sxl_fw']
verified successfully
VALID:   License for 'Acceleration' [mandatory feature 'sxl_ppk']
verified successfully
VALID:   License for 'Advanced Networking' [mandatory feature
'connect'] verified successfully
VALID:   License for 'Advanced Networking' [mandatory feature
'fgmodunl'] verified successfully
VALID:   License for 'Anti Virus' [mandatory feature 'av']
verified successfully
VALID:   License for 'Application Control' [optional feature
'appi'] verified successfully
VALID:   License for 'IPS-1' [optional feature 'ips'] verified
successfully
VALID:   License for 'URL Filtering' [optional feature 'urlf']
verified successfully
VALID:   License for 'Anti Bot' [mandatory feature 'abot']
verified successfully
VALID:   License for 'DLP' [optional feature 'dlp'] verified
successfully
VALID:   Same licenses are installed on all active blades
VALID:   No warnings in installed licenses
 successfully.
[Expert@SG-s01-01:0]#
```

asg log

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You can run the "`asg log`" command in Gaia gClish or in the Expert mode.
- You must run the "`show smo log`" command in Gaia gClish.

Description

Shows the content of log files aggregated from all Security Group Members.

Syntax in the Expert mode

```
asg log [-b <SGM IDs>] --file <Log File> [--from "<Timestamp>"] [--to "<Timestamp>"] [--tail <N>] [--filter "<String>"]
```

Syntax in Gaia gClish

```
show smo log <Log File> [from "<Timestamp>"] [to "<Timestamp>"] [tail <N>] [filter "<String>"]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

Parameter	Description
<Log File>	In the Expert mode, specifies the log file by its type or full path: ■ `audit` If you specify this 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` ■ `ports` If you specify this log type, the output shows all logs about ports in the `/var/log/` directory. To specify a log file, enter its full path and name. For example: `/var/log/ports` ■ `dist_mode` If you specify this 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 *"Working with the Distribution Mode" on page 554*.

Parameter	Description
	In Gaia gClish, specifies the log file by its type: ■ `acpid` Shows messages from the `/var/log/acpid` file. ■ `audit` Shows all audit messages from the `/var/log/` directory. ■ `auditlog` Shows messages from the `/var/log/audit/audit.log` file. ■ `auth` Shows messages from the `/var/log/auth` file. ■ `command_logger` Shows messages from the `/var/log/command_logger` file. ■ `cron` Shows messages from the `/var/log/cron` file. ■ `dist_mode` Shows all logs for the Distribution Mode activity. See *"Working with the Distribution Mode" on page 554*. ■ `gcopy` Shows all logs for the GCopy activity. ■ `gw_to_vsx` Shows messages from the Gateway to VSX Gateway conversion. ■ `messages` Shows messages from the `/var/log/messages*` file. ■ `pkg_config` Shows messages from the `/var/log/pkg_config_log` file. ■ `ports` Shows messages from the `/var/log/ports` file. ■ `routed` Shows messages from the `/var/log/routed*.log` file. ■ `save_config` Shows messages from the `/var/log/save_config_log` file. ■ `secure` Shows messages from the `/var/log/secure` file. ■ `send_alert` Shows messages from the `/var/log/send_alert` file. ■ `vs_start` Shows messages from the `/var/log/vs_start.elg` file.
`--from "<`*`Timestamp`*`>"`	Shows only the log entries from the specified timestamp and above. You must use the timestamp as it appears in the log file.

Parameter	Description
`--to "<Timestamp>"`	Shows only the log entries until the specified timestamp. You must use the timestamp as it appears in the log file.
`--tail <N>`	Show only the last `N` lines of the log file for each Security Group Member. For example, "`-tail 3`" shows only the last 3 lines of the specified log file. Default: 10 lines.
`--filter "<String>"`	Specifies a text string to use as a filter for the log entries. For example: `--filter debug`

Examples

Example 1 - messages on Site 1 that contain the word "Restarted"

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > show smo log messages filter Restarted
Feb 5 12:40:07 1_03 SG-s01-03 pm[8465]: Restarted /bin/routed[8489], count=1
Feb 5 12:40:09 1_04 SG-s01-04 pm[8449]: Restarted /bin/routed[9995], count=1
Feb 5 12:40:09 1_04 SG-s01-04 pm[8449]: Restarted /opt/CPsuite-R82/fw1/bin/cmd[11291], count=1
Feb 5 12:40:09 1_04 SG-s01-04 pm[8449]: Restarted /usr/libexec/gexecd[11292], count=1
Feb 5 12:40:10 1_03 SG-s01-03 pm[8465]: Restarted /usr/libexec/gexecd[9701], count=1
Feb 5 12:40:10 1_03 SG-s01-03 pm[8465]: Restarted /bin/routed[11328], count=2
Feb 5 12:40:10 1_05 SG-s01-05 pm[8458]: Restarted /bin/routed[9734], count=1
Feb 5 12:40:10 1_05 SG-s01-05 pm[8458]: Restarted /usr/libexec/gexecd[11331], count=1
Feb 5 12:40:11 1_01 SG-s01-01 pm[8463]: Restarted /bin/routed[12253], count=3
Feb 5 12:40:11 1_04 SG-s01-04 pm[8449]: Restarted /bin/routed[11378], count=2
Feb 5 12:40:11 1_04 SG-s01-04 pm[8449]: Restarted /opt/CPsuite-R82/fw1/bin/cmd[11379], count=2
[Global] SG-s01-01 >
```

Example 2 - Audit logs (specified by the log type)

```
[Expert@SG-s01-01:0]# 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_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@SG-s01-01:0]#
```

Example 3 - Port logs (specified by the log type), last 12 lines

```
[Expert@SG-s01-01:0]# asg log --file ports --tail 12
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-09 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-10 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-11 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-12 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-13 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-14 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-15 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-16 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-Mgmt1 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-Mgmt2 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-Mgmt3 link is down
Feb 3 18:01:40 2_05 SG-s02-05 cmd: Chassis 1 eth2-Mgmt4 link is down
[Expert@SG-s01-01:0]#
```

Example 4 - Port logs (specified by the full path), filtered by timestamps

```
[Expert@SG-s01-01:0]# 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 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-Mgmt1, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 SG-s01-02 cphaprob: Link state command ended successfully
[Expert@SG-s01-01:0]#
```

Example 5 - Distribution Mode logs (specified by the log type), filtered by the string "bridge"

```
[Expert@SG-s01-01:0]# asg log -b 1_01,1_04 --file dist_mode --filter "bridge"
Feb 2 18:10:30 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:10:30 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:12:31 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:12:31 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:14:14 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:14:14 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:14:30 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:14:30 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:16:19 1_01 SG-s01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
[Expert@SG-s01-01:0]#
```

Example 6 - '/var/log/messages' file, filtered by timestamps

```
asg log --file /var/log/messages --from "Oct 19 07:37:08" --to
"Oct 19 07:41:27"
```

asg_log_servers

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

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

```
asg_log_servers
```

Examples

```
[Expert@SG-s01-01:0]# 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 the 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    |  -                     |
|    13    |  -                     |
|    14    |  -                     |
+-----------------------------------+

("-" - Blade is not in Security Group)

Choose one of the following options:
-----------------------------------
1) Configure Log Servers Distribution mode
2) Exit
```

asg_lsp_util

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Enables or disables Link State Propagation (LSP) on the Security Group.

You must configure the required LSP Port Groups in the `/etc/lsp_groups.conf` file.

For more information, see *"Configuring Link State Propagation (LSP) on Scalable Chassis" on page 368*.

Syntax

```
asg_lsp_util
      -h
      enable
      disable
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`enable`	Enables Link State Propagation (LSP) on the Security Group.
`disable`	Disables Link State Propagation (LSP) on the Security Group.

Note - To restart the LSP mechanism, run:

1. `asg_lsp_util disable`
2. `asg_lsp_util enable`

asg_mac_resolver

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

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: ■ `0` - BMAC or SMAC ■ `1` - VMAC
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: ■ `0` - BMAC ■ `1` - SMAC
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 "`eth`*`X`*`-`*`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: ■ `0` - BMAC or SMAC ■ `1` - VMAC
2-3	ID of a Site. Limited to two ElasticXL Sites. Limited to two Maestro Sites. Limited to four Scalable Chassis.
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: ■ `0` - BMAC or SMAC ■ `1` - VMAC
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: ■ `0` - BMAC ■ `1` - SMAC
15	Always zero.
16	Sync interface. Possible values are: ■ `0` - Sync1 ■ `1` - Sync2

MAC Address Resolver

Description

Use the "`asg_mac_resolver`" command 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
- ID of the Site
- Security Group Member ID
- Assigned interface

Syntax

```
asg_mac_resolver <MAC address>
```

Examples

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Notes:

- The specified MAC Address comes from BPEth0 on Security Group Member #1 on 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 x.

asg_mac_verifier, mac_verifier

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run the "`asg_mac_verifier`" command in Gaia gClish.
- You must run the "`mac_verifier`" command in the Expert mode.

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.

Syntax in Gaia gClish

```
asg_mac_verifier -h
asg_mac_verifier [-l] [-v]
```

Syntax in the Expert mode

```
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 / Active Chassis.
`-v`	Shows information for each interface MAC Address.

Examples

Example 1

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example 2

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

asg monitor (on Security Groups)

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You can run this command in Gaia gClish or in the Expert mode.
- 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.

Description

Continuously shows the status of the Security Group and its components.

This command shows the same information as the command "*"asg stat" on page 829*", 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**.

The command output shows:

- Security Gateway Mode (Gateway or Legacy VSX)
- Number of Security Group Members in the Security Group
- Number of VSNextVirtual Gateways / Legacy VSXVirtual Systems
- Information related to VSNext / Legacy VSX configuration
- Uptime
- Software Version

Related Commands

- *"asg stat" on page 829*
- *"asg monitor (on Maestro Orchestrator)" on page 1001*

Syntax

```
asg monitor -h
asg monitor
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 `(local)` is the Security Group Member, on which you ran the command.

State	State of the Security Group Member:
	■ `ACTIVE`
	The Security Group Member is processing traffic.
	■ `DOWN`
	The Security Group Member is not processing traffic.
	■ `DETACHED/LOST`
	The Security Group Member is not communicating / during a reboot.
	■ `INIT`
	The Security Group Member is in the initialization phase after reboot.
	■ `READY`
	The Security Group Member is ready to become Active, and is waiting for all other remote Active members to acknowledge its state.
	■ `Active(Sync)`
	The Security Group Member is in a unicast connections sync.
	
	Note - To change the state of the Security Group Member manually, use these commands:
	■ In the Expert mode:
	`cluster-cli set members-admin-state ids <SGM ID> {up | down}`
	See *"cluster-cli" on page 863*.
	■ In Gaia gClish:
	`set cluster members-admin-state ids <SGM ID> {up | down}`
	See *"set cluster members-admin-state" on page 933*.

Examples

Example 1 - Shows the status of a Security Group Member (in Maestro)

```
[Expert@SG-s01-01:0]# asg monitor

-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                      | 12:03:48 hours                               |
| SGMs                         | 2 / 2                                        |
| Version                      | R82 (Build Number XX)                        |
| FW Policy Date               | 21Feb19 14:37                                |
| AMW Policy Date              | 21Feb19 14:37                                |
-------------------------------------------------------------------------------
| SGM ID                                Site 1                                |
|                                       ACTIVE                                |
-------------------------------------------------------------------------------
|  1                                      ACTIVE                              |
|  2                                      ACTIVE                              |
-------------------------------------------------------------------------------
```

Example 2 - Shows the component status in a Security Group (in Maestro)

```
[Expert@SG-s01-01:0]# asg monitor -v
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit        |        Chassis 1          |        Chassis 2          | Weight |
-------------------------------------------------------------------------------
| SGMs        |          3 / 3            |          3 / 3            |   6    |
| Ports       |                           |                           |        |
|   Standard  |          0 / 0            |          0 / 0            |  11    |
|   Bond      |          2 / 2            |          2 / 2            |  11    |
|   Other     |          0 / 0            |          0 / 0            |   6    |
| Sensors     |                           |                           |        |
|   SSMs      |          1 / 1            |          1 / 1            |  11    |
|             |                           |                           |        |
| Grade       |         51 / 51           |         51 / 51           |   -    |
-------------------------------------------------------------------------------
| Minimum grade gap for chassis failover:                            11       |
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
|     Sync to Standby chassis:   Enabled                                      |
-------------------------------------------------------------------------------
| Chassis HA mode:             Active Up                                      |
-------------------------------------------------------------------------------
```

Example 3 - Shows the component status on Scalable Chassis

```
[Expert@SG-s01-01:0]# 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     |                                                      |        |
|   Fans      |                        6 / 6                         |   5    |
|   SSMs      |                        2 / 2                         |  11    |
|   CMMs      |                        2 / 2                         |   6    |
|   PSUs      |                        5 / 5                         |   6    |
|             |                                                      |        |
| Grade       |                      205 / 205                       |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
```

asg_policy

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run the "`asg_policy`" command in the Expert mode.
- You can run the "`asg policy`" command in Gaia gClish or in the Expert mode.

Description

Shows the security policy status.

Controls the installed security policy.

Syntax in the Security Gateway / VSNext mode

```
asg_policy -h
asg policy -h
```

```
asg policy [-a] [--print_sig_diff]
      verify
      verify_amw
      unload [{--ip_forward |--disable_pnotes}]
```

Syntax in the Traditional VSX mode

```
asg_policy -h
asg policy -h
```

```
asg policy [-vs <VS ID>] [-a] [-v]
      verify
      verify_amw
      unload [--disable_pnotes]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Parameter	Description
`-vs <VS ID>`	Applies **only** to the Traditional VSX mode. Specifies the IDs of the relevant Virtual Systems. ■ If you do not enter the IDs, then the command applies to the current virtual context. ■ To specify one Virtual System ID, just enter its ID value. Example: `-vs 2` ■ To specify two or more Virtual System IDs, separate the ID values with the comma or the minus character. Example: `-vs 2,3` Example: `-vs 2-3` Example: `-vs 2,4-6`
`-a`	Applies the command also to the Security Group Members that are in the "DOWN" state.
`-v`	Applies **only** to the Traditional VSX mode. Verbose mode - shows the output for each Security Group Member.
`verify`	Verifies that the same Access Control policy is installed on all Security Group Members.
`verify_amw`	Verifies that the same Threat Prevention policy is installed on all Security Group Members.
`unload`	**Warning** - Do not use this command. For security reasons, your Security Group must always have a policy installed. Unloads the current security policy from all Security Group Members. ■ `--ip_forward` Enables the IP Forwarding in the Linux kernel. Does not apply to the Traditional VSX mode. **Warning** - This allows all traffic to pass through the Security Group without any inspection. ■ `--disable_pnotes` Configures the corresponding Critical Devices not to report their state as "`problem`".

Examples

Example 1 - Access Control policy

```
[Expert@SG-s01-01:0]# asg policy verify

+-------------------------------------------------------------------
-------+
|Policy Verification
      |
+-------+------------------+--------------+-----------------+-
-------+
|Member |Policy Name       |Policy Date    |Policy Signature
|Status  |
+-------+------------------+--------------+-----------------+-
-------+
|1_01   |Standard          |15Oct24 10:35  |21b8f0ef7
|Success |
|2_01   |Standard          |15Oct24 10:35  |21b8f0ef7
|Success |
+-------+------------------+--------------+-----------------+-
-------+


+-------------------------------------------------------------------
---------------+
|Summary
              |
+-------------------------------------------------------------------
---------------+
|Policy Verification completed successfully
              |
+-------------------------------------------------------------------
---------------+
[Expert@SG-s01-01:0]#
```

Example 2 - Threat Prevention Policy

```
[Expert@SG-s01-01:0]# asg policy verify_amw

+-------------------------------------------------------+
|AMW Policy Verification                                |
+-------+-------------------+-----------------+---------+
|Member |Policy Name        |Policy Signature |Status   |
+-------+-------------------+-----------------+---------+
|1_01   |Standard           |bd49c351c        |Success |
|2_01   |Standard           |bd49c351c        |Success |
+-------+-------------------+-----------------+---------+


+-------------------------------------------------------------------
---------------+
|Summary
               |
+-------------------------------------------------------------------
---------------+
|AMW Policy Verification completed successfully
               |
+-------------------------------------------------------------------
---------------+

[Expert@SG-s01-01:0]#
```

asg_mroute

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows this multicast routing information in a tabular format:

- **Source** - Source IP address
- **Dest** - Destination address
- **Iif** - Source interface
- **Oif** - Outbound interface

You can filter the output for specified interfaces and Security Group Members.

Related Commands

- *"asg_pim" on page 806*
- *"asg_igmp" on page 766*
- *"asg_route" on page 813*
- In Gaia gClish, run "`show route ...`"
- *"asg_dst_route" on page 735*

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 <Destination Route>`	Specifies the destination multicast group IP address.
`-s <Source Route>`	Specifies the source IP address.
`-i <Source Interface>`	Specifies the source interface name.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

Examples

Example 1 - Shows all multicast routes for all interfaces and Security Group Members

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

Example 2 - Shows only specific IP address, interfaces, destination IP address, or Security Group Members

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

asg_pim neighbors

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Shows the PIM neighbors.

Related Commands

- *"asg_pim" on page 806*

Syntax

```
asg_pim neighbors
      -h
      -b <SGM IDs>
      -i <Name of Interface>
      -n <PIM Neighbor>
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-i <Name of Interface>`	Specifies the interface.
`-n <PIM Neighbor>`	Specifies the PIM Neighbor.

asg_pim

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

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.

Related Commands

- *"asg_igmp" on page 766*
- *"asg_mroute" on page 801*
- *"asg_pim neighbors" on page 804*

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: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-i <if>`	Shows only the specified source interface.
`neighbors`	Runs verification tests to make sure that PIM `neighbors` are the same on all Security Group Members and shows this information: ■ **Verification** - Results of verification test ■ **Neighbor** - PIM neighbor ■ **Interface** - Interface name ■ **Holdtime** - Time in seconds to hold a connection open during peer negotiation ■ **Expires** - Minimum and Maximum expiration values for all Security Group Members
`-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@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

Example 2 - Shows PIM Information for the specific interface on all Security Group Members

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Example 3 - Shows PIM neighbors

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

asg_process_verifier

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Verifies the state of zombie processes on Security Group Members.

Syntax

```
asg_process_verifier
      -h
      -a
      -k [-y]
      -v
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`a`	Kills zombie processes and their parents. Use this parameter if the parameter "`-k`" cannot kill zombie processes.
`-k [-y]`	Kills zombie processes. The parameter "`-y`" does not ask for confirmation.
`-v`	Verifies that there are no zombie processes.

asg_provision

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Verifies the versions of Check Point software components on Security Group Members:

- Gaia OS version
- Software module consistency
- Hotfix consistency

Syntax

```
asg_provision
      -h
      no_version
      no_hotfix
      no_module
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`no_version`	Excludes the Gaia OS verification.
`no_hotfix`	Excludes the verification of software modules.
`no_module`	Excludes the verification of hotfixes.

asg_reboot

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

This command performs the software reboot.

Notes:

- At least one Security Group Member must be in the state "UP" to run this command.
- For Scalable Chassis:
  To learn how to restart an SSM from the CMM, see *"asg_chassis_ctrl" on page 1041*.

Related Commands

- *"cluster-cli" on page 863*
- *"set cluster members-reboot" on page 935*
- *"reboot" on page 917*

Syntax

```
asg_reboot
      -h
      -b <SGM IDs> [-a]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Runs the command on all Security Group Members.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-a`	Runs the command also on Security Group Members in the Administrative "DOWN" state.

Example

```
[Expert@SG-s01-01:0]# asg_reboot -b 1_03,2_05
You are about to perform hard reboot on SGMs: 1_03,2_05
It might cause performance hit for a period of time

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

Hard reboot requires auditing
Enter your full name: User1
Enter reason for hard reboot [Maintenance]:
WARNING: Hard reboot on SGMs: 1_03,2_05, User: User1, Reason:
Maintenance

Rebooting SGMs: 1_03,2_05
```

asg_route

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows routing information.

Related Commands

- *"asg_mroute" on page 801*
- In Gaia gClish, run "`show route ...`"
- *"asg_dst_route" on page 735*

Syntax

```
asg_route {-h | --help}
```

```
asg_route [-6] [-a] [-b <SGM IDs>] [--vs <VS ID>] [--summary] [--
compare-os-db]
      [{-i |--inactive} <Parameter>]
      [{-n |--dyn-route} <Parameter>]
      [{-r |--route} <Parameter>]
```

Parameters

Parameter	Description
`-h` `--help`	Shows the built-in help.
No Parameters	Shows all routes (IPv4 and IPv6).
`-6`	Shows only IPv6 routes.
`-a`	Includes the Security Group Members that are in the "DOWN" state.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`--vs <VS ID>`	Specifies the IDs of the Traditional VSX Virtual Systems. Applies to the Traditional Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.
`--summary`	Shows only a summary of all routes.
`--compare-os-db`	Shows only the inconsistency after it compares the routes between the Security Group database and the Gaia OS database.

Parameter	Description
`{-i |--inactive} <Parameter>`	Show only inactive routes. Valid `<Parameters>` are: ■ `all` - Shows all inactive routes. ■ `aggregate` - Shows only the aggregate routes. ■ `bgp` - Shows only the BGP routes. ■ `direct` - Shows only the directly connected routes. ■ `ospf` - Shows only the OSPF routes. ■ `static` - Shows only the static routes. ■ `rip` - Shows only the RIP routes.
`{-n |--dyn-route} <Parameter>`	Show only dynamic routes. Valid `<Parameters>` are: ■ `all` - Shows all dynamic routes. ■ `bgp` - Shows only the BGP routes. ■ `ospf` - Shows only the OSPF routes. ■ `rip` - Shows only the RIP routes.
`{-r |--route} <Parameter>`	Show only specified routes. Valid `<Parameters>` are: ■ `all` - Shows all routes. ■ `aggregate` - Shows only the aggregate routes. ■ `bgp` - Shows only the BGP routes. ■ `destination <IP Address>` - Shows only the route to the specified destination. ■ `direct` - Shows only the directly connected routes. ■ `exact <Network IP Address>` - Shows only the specific route. ■ `ospf` - Shows only the OSPF routes. ■ `rip` - Shows only the RIP routes. ■ `static` - Shows only the static routes. ■ `subnets <Network IP Address>` - Shows only the routes for the specified the network and its subnets.

Examples

Example 1 - Default output

```
[Expert@SG-s01-01:0]# asg_route
Collecting routing information, may take few seconds...
================================== VS
0=====================================

Fetching Routes info from Members:
1_01,1_02,1_03

-----------------------------------------------------
Status:  Routes info is identical on all Members
-----------------------------------------------------

Identical DB Routes: (7 records)
       NP - NAT Pool, U - Unreachable, i - Inactive
C              10.33.23.0/24       is directly connected, eth1-
Mgmt1
C              127.0.0.0/8         is directly connected, lo
C              192.0.2.0/24        is directly connected, Sync
C              198.51.101.0/25     is directly connected, eth1-
CIN
C              198.51.101.128/25   is directly connected, eth2-
CIN
S              0.0.0.0/0           via 10.33.23.1, eth1-Mgmt1,
active


Types: C - Connected, S - Static, R - RIP, B - BGP,
       O - OSPF IntraArea (IA - InterArea, E - External, N -
NSSA)
       A - Aggregate, K - Kernel Remnant, H - Hidden, P -
Suppressed
       SBR - Source-Based Routes

-----------------------------------------------------
Identical UIPS for Site 1 Routes: (0 records)
UIPS is disabled on Site 1


*************************************************************
*********
Summary of inconsistent DB routes:: no inconsistent routes found

*************************************************************
*********
```

```
================================================================
===============
================================== VS
1=====================================

Fetching Routes info from Members:
1_01,1_02,1_03

------------------------------------------------------
Status:  Routes info is identical on all Members
------------------------------------------------------

Identical DB Routes: (5 records)
       NP - NAT Pool, U - Unreachable, i - Inactive
C               10.34.200.0/24      is directly connected, bond3
C               127.0.0.0/8         is directly connected, lo
C               192.168.34.0/24     is directly connected,
bond2.34
S               0.0.0.0/0           via 192.168.34.1, bond2.34,
active


Types: C - Connected, S - Static, R - RIP, B - BGP,
       O - OSPF IntraArea (IA - InterArea, E - External, N -
NSSA)
       A - Aggregate, K - Kernel Remnant, H - Hidden, P -
Suppressed
       SBR - Source-Based Routes

------------------------------------------------------
Identical UIPS for Site 1 Routes: (0 records)
UIPS is disabled on Site 1


**************************************************************
*********
Summary of inconsistent DB routes:: no inconsistent routes found

**************************************************************
*********


================================================================
===============
```

Example 2 - Only the summary

```
[Expert@SG-s01-01:0]# asg_route --summary
Collecting routing information, may take few seconds...
================================== VS
0=====================================

Fetching Summary info from Members:
1_01,1_02,1_03

-----------------------------------------------------
Status:  Summary info is identical on all Members
-----------------------------------------------------

Identical DB Summary: (10 records)
Total            6
aggregate        0
bgp              0
connected        5
igrp             0
isis             0
kernel           0
nat-pool         0
rip              0
static           1


-----------------------------------------------------
Identical UIPS for Site 1 Summary: (0 records)
UIPS is disabled on Site 1


*************************************************************
*********
Summary of inconsistent DB routes:: no inconsistent routes found

*************************************************************
*********


=============================================================
===============
================================== VS
1=====================================

Fetching Summary info from Members:
```

```
1_01,1_02,1_03

------------------------------------------------------
Status:  Summary info is identical on all Members
------------------------------------------------------

Identical DB Summary: (10 records)
Total             4
aggregate         0
bgp               0
connected         3
igrp              0
isis              0
kernel            0
nat-pool          0
rip               0
static            1


------------------------------------------------------
Identical UIPS for Site 1 Summary: (0 records)
UIPS is disabled on Site 1


**************************************************************
*********
Summary of inconsistent DB routes:: no inconsistent routes found

**************************************************************
*********


==============================================================
================

[Expert@SG-s01-01:0]#
```

Example 3 - Show all the routes to the network 8.0.0.0/8 and its subnets

```
[Expert@SG-s01-01:0]# asg_route --route subnets 8.0.0.0
```

Example 4 - Show OSPF neighbours

```
[Expert@SG-s01-01:0]# asg_route -n ospf
```

add smo

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Adds settings related to the Single Management Object (SMO) on the Security Group.

Important - Do **not** use this command, unless Check Point Support or an Administration Guide explicitly tells you to do so.

Related Commands

- *"show smo" on page 990*
- *"set smo" on page 954*
- *"delete smo" on page 886*

Syntax

```
add smo
      security-group <SGM IDs>
      user-defined sync-file <Path and Name of File>
```

Commands

Command	Description
`add smo security-group <SGM IDs>`	Applies only to Scalable Chassis that has one Security Group. Adds the specified Security Group Members to the Security Group. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`add smo user-defined sync-file <Path and Name of File>`	Adds the specified file for synchronization from the SMO. The command saves the specified files in this file: `/etc/xfer_file_list.user`

Examples

```
[Expert@SG-s01-01:0]# touch /var/tmp/test.txt
[Expert@SG-s01-01:0]#

[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01>
[Global] SG-s01-01> add smo user-defined sync-file
/var/tmp/test.txt
>>> current vrf is 0
>>> current vrf is 0
>>> current vrf is 0

Updating synced file list...
Operation completed successfully

Copying /var/tmp/test.txt to all SGMs...
Operation completed successfully

[Global] SG-s01-01>
[Global] SG-s01-01> show smo user-defined sync-file
>>> current vrf is 0
>>> current vrf is 0
>>> current vrf is 0

+-------------------------------------------------------------+
|Synced Files                                                 |
+-------------------------------------------------------------+
|File name                                                    |
+-------------------------------------------------------------+
|/var/tmp/test.txt                                            |
+-------------------------------------------------------------+

[Global] SG-s01-01>
[Global] SG-s01-01> delete smo user-defined sync-file [PRESS TAB
TO SEE FILES]
[Global] SG-s01-01> delete smo user-defined sync-file
/var/tmp/test.txt
>>> current vrf is 0
>>> current vrf is 0
>>> current vrf is 0

Updating synced file list...
Operation completed successfully

100% /etc/xfer_file_list.user
100% /etc/xfer_file_list.user
Operation completed successfully
```

```
[Global] SG-s01-01>
```

asg stat

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You can run this command in Gaia gClish or in the Expert mode.
- If you run this command in the context of a VSNext Virtual Gateway / Legacy VSX Virtual System, the output applies only to that Virtual Gateway / Legacy Virtual System.

Description

Show the state of the Security Group and its hardware components.

To show this output continuously, use the "*"asg monitor (on Security Groups)" on page 792*" command.

The command output shows:

- Security Gateway Mode (Gateway or Traditional VSX)
- Number of Security Group Members in the Security Group
- Number of VSNext Virtual Gateways / Traditional VSX Virtual Systems
- Information related to VSNext / Traditional VSX configuration
- Uptime
- Software Version

Related Commands

- *"asg monitor (on Security Groups)" on page 792*

Syntax

```
asg stat
      -h
      -i list_all
      -i sgm_info
      -i tasks
      -v [-amw]
      vs [all [-p]]
```

Parameters

Parameter	Description
No Parameters	Shows the Security Group status (short output).
`-h`	Shows the built-in help.
`-i list_all`	Shows: ■ The IDs of the Security Group Members, their state and IP addresses ■ Tasks and on which Security Group Member they run
`-i sgm_info`	Shows the IDs of the Security Group Members, their state and IP addresses
`-i tasks`	Shows the list of Tasks and on which Security Group Member they run: ■ **SMO** - Single Management Object ■ **General** - General ■ **LACP** - Interface Bonding ■ **CH Monitor** - Site state monitor ■ **DR Manager** - Dynamic Routing manager ■ **UIPC** - Unique IP Address per Site (formerly, Unique IP Address per Chassis, UIPC) • For Maestro Dual Site, see *"Configuring a Unique IP Address per Site (UIPS) in Maestro Dual Site" on page 208*. • For Scalable Chassis Dual Chassis, see *"Configuring a Unique IP Address per Site (UIPS) in Dual Chassis" on page 389*. ■ **Alert** - Alerts
`-v [-amw]`	Shows the detailed Security Group status (verbose output). The "`-amw`" parameter shows the update status for the applicable Software Blades.

Parameter	Description
`vs [all [-p]]`	Shows the VSX information: ■ `vs` Shows a general output for a Virtual System. Run this command in the context of the applicable Virtual System. ■ `vs all` Output also shows all Virtual Systems and their states. ■ `vs all -p` Output also shows all Virtual Systems and a summary sentences for the health status instead of shows the state of each Virtual System. For more information on a specific Virtual System, run the "`asg stat vs`" command in the context of the Virtual System.

Examples

Example 1 - Default Output (asg stat)

Syntax

```
asg stat
```

Example output of "`asg stat`" from a Maestro Single Site configuration

```
[Expert@SG-s01-01:0]# asg stat
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 02:10:27 hours                                |
| Members                     | 2/2                                           |
| Version                     | R82 (Build Number XXX)                        |
-------------------------------------------------------------------------------
| Site Parameters                                                             |
-------------------------------------------------------------------------------
| Unit         |                           Site1                            |
-------------------------------------------------------------------------------
| Members      |                             2 / 2                          |
| Ports        |                             2 / 2                          |
| SSMs         |                             2 / 2                          |
-------------------------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

Example output of "`asg stat`" from a Maestro Dual Site configuration

```
[Expert@SG-s01-01:0]# asg stat
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Cluster Mode                | Active Up                                     |
| Up time                     | 21:29:56 hours                                |
| Members                     | 12/12                                         |
| Version                     | R82 (Build Number XXX)                        |
-------------------------------------------------------------------------------
| Site Parameters                                                             |
-------------------------------------------------------------------------------
| Unit         |          Site1                |          Site2               |
-------------------------------------------------------------------------------
| Members      |            6 / 6              |            6 / 6             |
| Ports        |            5 / 5              |            5 / 5             |
| SSMs         |            2 / 2              |            2 / 2             |
-------------------------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

Example 2 - Detailed Output (asg stat -v)

Syntax

```
asg stat -v
```

Example output of "`asg stat -v`" from a Maestro Single Site configuration

This output shows a Security Group with 6 Security Group Members in the Active (UP) state (out of total 6).

```
[Expert@SG-s01-01:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 02:10:39 hours                                |
| Members                     | 6/6                                           |
| Version                     | R82 (Build Number XXX)                       |
-------------------------------------------------------------------------------
| Member ID                            Site1                                  |
|                                      ACTIVE                                 |
-------------------------------------------------------------------------------
|  1                                  ACTIVE                                  |
|  2                                  ACTIVE                                  |
|  3                                  ACTIVE                                  |
|  4                                  ACTIVE                                  |
|  5                                  ACTIVE                                  |
|  6                                  ACTIVE                                  |
-------------------------------------------------------------------------------
| Site Parameters                                                             |
-------------------------------------------------------------------------------
| Unit        |                     Site1                          | Weight |
-------------------------------------------------------------------------------
| Members     |                        6 / 6                       |   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 site:       Enabled                                      |
-------------------------------------------------------------------------------
```

Example output of "`asg stat -v`" from a Maestro Dual Site configuration

This output shows a Security Group with 6 Security Group Members in the Active (UP) state (out of total 6).

The Maestro Site #1 is Active.

The Maestro Site #2 is Standby.

```
[Expert@SG-s01-01:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Cluster Mode                | Active Up                                     |
| Up time                     | 5 days, 21:23:47 hours                        |
| Members                     | 6/6                                           |
| Version                     | R82 (Build Number XXX)                       |
-------------------------------------------------------------------------------
| Member ID             Site1                              Site2               |
|                       ACTIVE                             STANDBY             |
-------------------------------------------------------------------------------
|  1                   ACTIVE                             ACTIVE               |
|  2                   ACTIVE                             ACTIVE               |
|  3                   ACTIVE                             ACTIVE               |
|  4                   ACTIVE                             ACTIVE               |
|  5                   ACTIVE                             ACTIVE               |
|  6                   ACTIVE                             ACTIVE               |
-------------------------------------------------------------------------------
| Site Parameters                                                             |
-------------------------------------------------------------------------------
| Unit        |        Site1              |        Site2              | Weight |
-------------------------------------------------------------------------------
| Members     |          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 site failover:                                  11    |
| Synchronization                                                             |
|     Sync to Active site:       Enabled                                      |
|     Sync to Standby site:      Enabled                                      |
-------------------------------------------------------------------------------
| Site HA mode:                Active Up                                      |
-------------------------------------------------------------------------------
```

Example output of "`asg stat -v`" from an ElasticXL Cluster Dual Site configuration

This output shows a Security Group with 6 Security Group Members in the Active (UP) state (out of total 6).

The Site #1 is Active.

The Site #2 is Standby.

```
[Expert@SG-s01-01:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - ElasticXL                                                   |
-------------------------------------------------------------------------------
| Cluster Mode                | Active Up                                     |
| Up time                     | 75 days, 09:36:13 hours                       |
| Members                     | 6 / 6                                         |
| Version                     | R82 (Build Number XXX)                        |
-------------------------------------------------------------------------------
| Member ID             Site1                              Site2              |
|                       ACTIVE                             STANDBY            |
-------------------------------------------------------------------------------
|  1                   ACTIVE                             ACTIVE              |
|  2                   ACTIVE                             ACTIVE              |
|  3                   ACTIVE                             ACTIVE              |
-------------------------------------------------------------------------------
| Site Parameters                                                             |
-------------------------------------------------------------------------------
| Unit        |        Site1              |        Site2              | Weight |
-------------------------------------------------------------------------------
| Members     |          3 / 3            |          3 / 3            |   6    |
|             |                           |                           |        |
| Grade       |         18 / 18           |         18 / 18           |   -    |
-------------------------------------------------------------------------------
| Minimum grade gap for site failover:                                   6    |
| Synchronization                                                             |
|     Sync to Active site:       Enabled                                      |
|     Sync to Standby site:      Enabled                                      |
-------------------------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

Explanation about the output:

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 **Members** line, "6 / 6" means that there are currently 6 Security Group Members in the state "UP" out of the 6 that must be in the state "UP".

Field	Instructions
Member ID	Identifier of the Security Group Member. The (local) is the Security Group Member, on which you ran the command.

Field	Instructions

State	State of the Security Group Member:
	■ `ACTIVE`
	The Security Group Member is processing traffic.
	■ `DOWN`
	The Security Group Member is not processing traffic.
	■ `DETACHED/LOST`
	The Security Group Member is not communicating / during a reboot.
	■ `INIT`
	The Security Group Member is in the initialization phase after reboot.
	■ `READY`
	The Security Group Member is ready to become Active, and is waiting for all other remote Active members to acknowledge its state.
	■ `Active(Sync)`
	The Security Group Member is in a unicast connections sync.
	Note - To change the state of the Security Group Member manually, use these commands:
	■ In the Expert mode:
	`cluster-cli set members-admin-state ids <SGM ID> {up | down}`
	See *"cluster-cli" on page 863*.
	■ In Gaia gClish:
	`set cluster members-admin-state ids <SGM ID> {up | down}`
	See *"set cluster members-admin-state" on page 933*.

Field	Instructions

Grade	The sum of the grades of all components.
	The grade of each component is the unit weight multiplied by the number of components that are in the state "`UP`".
	You can configure the unit weight of each component to show the importance of the component in the system.
	To configure the unit weight, run in Gaia gClish:
	`set cluster configuration high-availability factors <Hardware Component>`
	For example, to change the weight of the Security Group Member to 12, run in Gaia Clish on that Security Group Member:
	`set cluster configuration high-availability factors member 12`
	See:
	■ For Maestro - *"Configuring Security Group High Availability in Maestro" on page 255*.
	■ For Scalable Chassis - *"Configuring Scalable Chassis High Availability" on page 374*.
	If you run the "`asg stat -v`" command, the output shows a greater unit weight and system grade.

Minimum grade gap for chassis failover	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. Minimum threshold for traffic processing - the minimum grade required for the Site to become Active.
Synchronization	Status of synchronization between Security Group Members: ■ Within a Site - between Security Group Members located in the same Security Group. ■ Between two Sites - between Security Group Members located on different Sites.

Example 3 - List of Tasks (asg stat -i tasks)

Syntax

```
asg stat -i tasks
```

Example output of "`asg stat -i tasks`" from a Security Group in a Maestro Single Site configuration

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

```
[Expert@SG-s01-01:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)    |                      Site1                              |
-------------------------------------------------------------------------------
| 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@SG-s01-01:0]#
```

Example output of "`asg stat -i tasks`" from a Security Group in a Maestro 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@SG-s01-01:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Site1               |        Site2               |
-------------------------------------------------------------------------------
| 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@SG-s01-01:0]#
```

Example output of "`asg stat -i tasks`" from all Security Group Members (in our example, there are two on each Site):

```
[Expert@SG-s01-01:0]# g_all asg stat -i tasks
1_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Site1               |        Site2               |
-------------------------------------------------------------------------------
| 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)     |        Site1               |        Site2               |
-------------------------------------------------------------------------------
| 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)     |        Site1               |        Site2               |
-------------------------------------------------------------------------------
| 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)     |        Site1               |        Site2               |
-------------------------------------------------------------------------------
| 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@SG-s01-01:0]#
```

Example 4 - Traditional VSX Information for the current Legacy Virtual System (asg stat vs)

Syntax

```
asg stat vs
```

Example output of "`asg stat vs`" from a Maestro Dual Site configuration - context of VS #1

```
[Expert@SG-s01-01:0]# asg stat
-------------------------------------------------------------------------------
| VSX System Status - Maestro                                                 |
-------------------------------------------------------------------------------
| VS ID                    1                                                  |
| VS Name                  MyVirtualSystem                                    |
| Cluster Mode             Active Up                                          |
| Software Blades          N/A                                                |
| FW Policy Date           09Oct24 05:46                                      |
| AMW Policy Date          N/A                                                |
-------------------------------------------------------------------------------
| Site Parameters                                                             |
-------------------------------------------------------------------------------
| Unit         |          Site1                |          Site2                |
-------------------------------------------------------------------------------
| Ports        |            1 / 1              |            1 / 1              |
| FWKs         |            1 / 1              |            1 / 1              |
| Member       |            1 / 1              |            1 / 1              |
-------------------------------------------------------------------------------
[Expert@SG-s01-01:0]#
```

Example 6 - Traditional VSX Information for all Legacy Virtual Systems (asg stat vs all)

Syntax

```
asg stat vs all
```

Example output of "`asg stat vs all`" from a Maestro Dual Site configuration

```
[Expert@SG-s01-01:0]# asg stat vs all
-------------------------------------------------------------------------------------------------
| VSX System Status - Maestro                                                                   |
-------------------------------------------------------------------------------------------------
| Cluster Mode                            | Active Up                                           |
| Up time                                 | 5 days, 21:51:58 hours                              |
| Members                                 | 2 / 2                                               |
| Virtual Systems                         | 3                                                   |
| Version                                 | R82 (Build Number XXX)                              |
-------------------------------------------------------------------------------------------------
| VSID | VS Type & Name        | Site1             | Site2             | Health            |
-------------------------------------------------------------------------------------------------
| 0    | V MyVirtualSystem     | STANDBY           | ACTIVE            | OK                |
| 1    | S MyVirtualSwitch     | STANDBY           | ACTIVE            | OK                |
-------------------------------------------------------------------------------------------------
| Active Virtual Systems       | 0                | 2                 |                   |
-------------------------------------------------------------------------------------------------
| Synchronization                                                                               |
|     Sync to Active site:       Enabled                                                        |
|     Sync to Standby site:      Enabled                                                        |
-------------------------------------------------------------------------------------------------

(P) - VS Primary site

For more information on a specific VS: run "asg stat vs" from VS context.

[Expert@SG-s01-01:0]#
```

asg_swb_update_verifier

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You can run this command in Gaia gClish or in the Expert mode.
- In the VSNext mode, you must run this command in the context of the applicable Virtual Gateway.

Description:

Verifies the update status for these Software Blades:

- Anti-Bot
- Anti-Virus
- Application Control
- URL Filtering

Syntax:

```
asg_swb_update_verifier
      {-h | --help}
      {-v | --verbose}
      -b <SGM IDs>
      {-c | --cert} <Certificate File>
      -m <Product> [-n]
      -p <Proxy IP Address>[:<Proxy Port Number>]
      -u <Product>
      --vs <VS ID>
```

Parameters:

Parameter	Description
`-h` `--help`	Shows the built-in help.

Parameter	Description
`-v` `--verbose`	Shows verbose output.
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-c <Certificate File>` `--cert <Certificate File>`	Specifies the SSL certificate file for the online update.

Parameter	Description
`-m <Product> [-n]`	Pushes the database from the local Security Group Member (on which you run this command) and applies it to the Security Group Members specified in the "`-b`" option. By default, applies to all Security Group Members. The "`-n`" option forces the online update before the push operation. This online update uses the default proxy server in Gaia OS, unless you specify the "`-p`" option. Valid "`<Product>`" values: ■ `all` This is the default. Applies to all supported Software Blades (see the description section above). ■ `Anti-Bot` Applies only to the Anti-Bot Software Blade. ■ `Anti-Virus` Applies only to the Anti-Virus Software Blade. ■ `APPI` Shows the output only for the Application Control Software Blade. ■ `URLF` Applies only to the URL Filtering Software Blade.
`-p <Proxy IP Address>[:<Proxy Port Number>]`	Specifies the proxy server for the online update.
`-u <Product>`	Specifies the Software Blade, for which to run this command. Valid "`<Product>`" values: ■ `all` This is the default. Applies to all supported Software Blades (see the description section above). ■ `Anti-Bot` Applies only to the Anti-Bot Software Blade. ■ `Anti-Virus` Applies only to the Anti-Virus Software Blade. ■ `APPI` Shows the output only for the Application Control Software Blade. ■ `URLF` Applies only to the URL Filtering Software Blade.

Parameter	Description
`--vs <VS ID>`	Specifies the IDs of the Traditional VSX Virtual Systems. Applies to the Traditional Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.

Examples

Example 1 - Show the current database status

In this example, there are three Security Group Members.

```
[Expert@SG-s01-01:0]# asg_swb_update_verifier
+-----------------------------------------------------------------
---------------+
| product    | member | status           | DB version | next
update check        |
+-----------------------------------------------------------------
---------------+
| APPI       | 1_01 | not-installed    | N/A        | N/A
             |
| APPI       | 1_02 | not-installed    | N/A        | N/A
             |
| APPI       | 1_03 | not-installed    | N/A        | N/A
             |
| Anti-Bot   | 1_01 | not-installed    | N/A        | N/A
             |
| Anti-Bot   | 1_02 | not-installed    | N/A        | N/A
             |
| Anti-Bot   | 1_03 | not-installed    | N/A        | N/A
             |
| Anti-Virus | 1_01 | not-installed    | N/A        | N/A
             |
| Anti-Virus | 1_02 | not-installed    | N/A        | N/A
             |
| Anti-Virus | 1_03 | not-installed    | N/A        | N/A
             |
| URLF       | 1_01 | not-installed    | N/A        | N/A
             |
| URLF       | 1_02 | not-installed    | N/A        | N/A
             |
| URLF       | 1_03 | not-installed    | N/A        | N/A
             |
+-----------------------------------------------------------------
---------------+

Report:
------------------------------ APPI ----------------------------
----------------
DB versions verification
     [   OK   ]
statuses verification
     [   OK   ]

------------------------------ 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   ]

[Expert@SG-s01-01:0]#
```

Example 2 - Manually update the Anti-Bot Software Blade on the Security Group Member 1_2 in the Legacy Virtual System 3

```
[Expert@SG-s01-01:0]# asg_swb_update_verifier -b 1_2 -m Anti-Bot
--vs 3
```

Example 3 - Manually update the Anti-Virus Software Blade on the Security Group Member 1_3, perform online update

```
[Expert@SG-s01-01:0]# asg_swb_update_verifier -b 1_3 -m Anti-
Virus -n
```

asg_tracert

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Show the `tracert` results on the Security Group.

The native Linux "`tracert`" utility cannot handle the "`tracert`" pings correctly because of the stickiness mechanism used in the Security Group Firewall.

The "`asg_tracert`" command supports all options and parameters of the native Linux "`tracert`" utility.

Syntax

```
asg_tracert <IP Address> [<tracert Options>]
```

Parameters

Parameter	Description
<IP Address>	Specifies the destination IP address.
<tracert Options>	Specifies the native `tracert` command options.

Examples

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

asg_unique_mac_utility

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Use the "`asg_unique_mac_utility`" command to configure these:

- Data interface Unique MAC Identifier
- Host name

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 "`eth`*`X`*`-`*`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.

Procedure

Step	Instructions
1	Connect to the command line on the Security Group.
2	Run this command: `asg_unique_mac_utility`

3	Select an option from the menu and follow the instructions on the screen.
	Example:
	`----------------------------------------------`
	`| 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`

4	Reboot the Security Group to apply the new Unique MAC Identifier: `reboot -b all`

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`.

asg_vsx_verify

This command is supported only on these:

- Maestro Security Group in the Traditional VSX mode
- Scalable Chassis Security Group in the Traditional VSX mode

Notes:

- You must run the "`asg_vsx_verify`" command in the Expert mode
- You can run the "`asg vsx_verify`" command in Gaia gClish or in the Expert mode

Description

Confirms that all Security Group Members have the same Traditional 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-R82/fw1/conf/fwha_vsx_conf_id.conf
+b21dfa3feab817c3640bbb984346cdf1  /opt/CPsuite-R82/fw1/conf/fwha_vsx_conf_id.conf
```

Syntax in the Expert mode

```
asg_vsx_verify [{-a | -c | -v}]
asg vsx_verify [{-a | -c | -v}]
```

Syntax in Gaia gClish

```
asg vsx_verify [{-a | -c | -v}]
```

Parameters

Parameter	Description
`-a`	Includes Security Group Members in the Administrative DOWN state
`-c`	Compares: ■ Database configuration between Security Group Members ■ Operating system and database configuration on each Security Group Member
`-v`	Includes Virtual Systems configuration verification table

Examples

Example 1 - 'asg vsx_verify -v'

```
[Expert@SG-s01-01:0]# asg vsx_verify -v
+------------------------------------------------------------------------------+
|Site 1 members:                                                               |
|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 DB. 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
[Expert@SG-s01-01:0]#
```

Example 2 - 'asg vsx_verify -a -v'

```
[Expert@SG-s01-01:0]# asg vsx_verify -v -a
Output
+------------------------------------------------------------------------------+
|Site 1 members:                                                               |
|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 DB. 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
[Expert@SG-s01-01:0]#
```

clock_verifier

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Verifies the time skew between Security Group Members.

Syntax

```
clock_verifier -v
```

Examples

Example 1 - From a Maestro Security Group

```
[Expert@SG-s01-01:0]# clock_verifier -v
-*- 1 blade: 1_01 -*-
Sun Oct 20 20:33:08 IDT 2024
-*- 2 blades: 1_02 2_02 -*-
Sun Oct 20 20:33:05 IDT 2024
-*- 1 blade: 1_03 -*-
Sun Oct 20 20:33:19 IDT 2024
-*- 1 blade: 2_01 -*-
Sun Oct 20 20:33:18 IDT 2024
-*- 1 blade: 2_03 -*-
Sun Oct 20 20:33:22 IDT 2024

system is virtual. skipping CMM skew test...

Skew is 18 seconds

[Expert@SG-s01-01:0]#
```

Example 2 - From a Scalable Chassis

```
[Expert@SG-s01-01:0]# clock_verifier -v
-*- 2 blades: 1_01 1_02 -*-
Sun Oct 20 20:30:14 IDT 2024
-*- 2 blades: 1_03 1_04 -*-
Sun Oct 20 20:30:15 IDT 2024
-*- 1 blade: 1_05 -*-
Sun Oct 20 20:30:13 IDT 2024
-*- 1 blade: 2_01 -*-
Sun Oct 20 20:30:19 IDT 2024
-*- 4 blades: 2_02 2_03 2_04 2_05 -*-
Sun Oct 20 20:30:17 IDT 2024

Chassis 1: CMM time is Sun Oct 20 20:30:15 IDT 2024
Chassis 2: CMM time is Sun Oct 20 20:30:20 IDT 2024

Skew is 6 seconds
[Expert@SG-s01-01:0]#
```

cluster-cli

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

- Shows cluster information.
- Controls the administrative state of Security Group Members on the specified Site.
- Controls the administrative state of the specified Site.

Related Commands

- *"cluster_site_admin" on page 874*
- *"set cluster sites-admin-state" on page 937*
- *"set cluster site-id <Site ID> admin-state" on page 939*
- *"set cluster members-admin-state" on page 933*
- *"set cluster members-reboot" on page 935*
- *"asg_reboot" on page 811*

Syntax

```
cluster-cli --help
```

```
cluster-cli set [-f {json [-p] | widget}]
      members-admin-state
            ids <SGM ID> {up | down}
            local {up | down}
            remote {up | down}
      members-reboot
            ids <Site ID>
            local
            remote}
      sites-admin-state
            ids <Site ID> {up | down}
            local {up | down}
            remote {up | down}
```

```
cluster-cli show [-f {json [-p] | widget}]
            info [-l]
                  connection [--sip <Source IP Address>] [--dip
<Destination IP Address>] [--sport <Source Port>] [--dport
<Destination Port>] [--proto <Protocol Number>]
                  cpu
                  interfaces
                  overview
                  pnotes
                  policy
                  provision
                  throughput
```

```
cluster-cli tui
```

Shortened commands:

- The command "`cset`" is the alias for the command "`cluster-cli set`"
- The command "`cinfo`" is the alias for the command "`cluster-cli show info`"
- The command "`cconn`" is the alias for the command " `cluster-cli show info connection`"
- The command "`cstat`" is the alias for the command "`cluster-cli show info overview`"

Parameters

Parameter	Description
`--help`	Shows the built-in help.
`-f {json [-p] | widget}` `--format {json [-p] | widget}`	Specifies the output format: ■ `json [-p]` - JSON (the parameter "-p" show the "pretty" JSON) ■ `widget` - tabular format (this is the default)
`cluster-cli set members-admin-state`	Configures the administrative state of the specified Security Group Members (up or down). For Gaia gClish, see *"set cluster members-admin-state" on page 933*. ■ `cluster-cli set members-admin-state ids <SGM ID> {up | down}` Configures the administrative state (up or down) of the specified Security Group Members. `<SGM IDs>` can be: • One Security Group Member (for example, `1_1`) • A comma-separated list of Security Group Members (for example, `1_1,1_4`) • A range of Security Group Members (for example, `1_1-1_4`) ■ `cluster-cli set members-admin-state local {up | down}` Configures the administrative state (up or down) of all all Security Group Members on the local Site (to which you are connected). ■ `cluster-cli set members-admin-state remote {up | down}` Configures the administrative state (up or down) of all Security Group Members on the remote Site.

Parameter	Description
`cluster-cli set members-reboot`	Reboots all Security Group Members on the specified Site. For Gaia gClish, see *"set cluster members-reboot" on page 935*. ■ `cluster-cli set members-reboot ids <SGM ID>` Reboots the specified Security Group Members. `<SGM IDs>` can be: • One Security Group Member (for example, `1_1`) • A comma-separated list of Security Group Members (for example, `1_1,1_4`) • A range of Security Group Members (for example, `1_1-1_4`) ■ `cluster-cli set members-reboot local}` Reboots all Security Group Members on the local Site, to which you are currently connected. ■ `cluster-cli set members-reboot remote}` Reboots all Security Group Members on the remote Site.
`cluster-cli set sites-admin-state`	Configures the administrative state of the entire Site (up or down). For Gaia gClish, see *"set cluster sites-admin-state" on page 937*. ■ `cluster-cli set sites-admin-state ids <Site ID> {up | down}` Configures the administrative state (up or down) of the entire specified Site: • `1` - Applies to Site #1 • `2` - Applies to Site #2 ■ `cluster-cli set sites-admin-state local {up | down}` Configures the administrative state (up or down) of the local Site (to which you are connected). ■ `cluster-cli set sites-admin-state remote {up | down}` Configures the administrative state (up or down) of the remote Site.
`cluster-cli show info [-l]`	Shows cluster configuration. The parameter "`-l`" shows continuous (live) output. For Gaia gClish, see *"show cluster info" on page 967*.

Parameter	Description
`cluster-cli show info connection [<Parameters>]`	Shows the current cluster connections.
`cluster-cli show info [-l] cpu`	Shows the CPU usage and the roles of the CPU cores.
`cluster-cli show info [-l] interfaces`	Shows information about the cluster interfaces: ■ Name ■ IP Address ■ Driver name ■ State ■ Throughput ■ Packet rate
`cluster-cli show info [-l] overview`	Shows the cluster overview information: ■ State of each Site ■ State of each Security Group Member ■ Throughput ■ Packet rate ■ Connection rate ■ Number of concurrent connections ■ Overall CPU usage ■ CoreXL split (Firewall instances / SND instances) ■ Overall CPU usage for CoreXL Firewall instances and SND instances ■ RAM usage ■ Which Critical Devices report their state as "`problem`" ■ State of Heart Beat
`cluster-cli show info [-l] pnotes`	Shows the Critical Devices that report their state as "`problem`".
`cluster-cli show info [-l] policy`	Shows information about the installed policy.
`cluster-cli show info [-l] provision`	Shows the provisioning state of new Security Group Members. You can see the progress if there are new Security Group Members that are joining the Security Group.
`cluster-cli show info [-l] throughput`	Shows the traffic throughput for the Management Interfaces and the Sync Interfaces.

Parameter	Description
`cluster-cli tui`	Opens the Textual UI: 1. In the left panel, click the required command. 2. In the top right panel, click the required option. 3. In the bottom right panel, examine the syntax. 4. Press the **CTRL +R** keys to close the TUI and run the selected command To close the TUI without running a command, press the **CTRL +C** or **CTRL +D** keys.

Examples

Example 1 - 'cluster-cli show info cpu'

```
[Expert@SG-s01-01:0]# cluster-cli show info cpu
Member 1_01

┌──────────┬──────────┬──────────┬──────────┬──────────┬──────────┬
──────────┬──────────┬──────────┬──────────┬──────────┐
│ Range/IDX │ 0        │ 1        │ 2        │ 3        │ 4        │
5        │ 6        │ 7        │ 8        │ 9        │

├──────────┼──────────┼──────────┼──────────┼──────────┼──────────┼
──────────┼──────────┼──────────┼──────────┼──────────┤
│ 0-9       │ [S] 1    │ [S] 0    │ [S] 0    │ [S] 1    │ [F] 7    │
[F] 12   │ [F] 8    │ [F] 7    │ [F] 6    │ [F] 9    │
│ 10-19     │ [S] 1    │ [S] 0    │ [S] 0    │ [S] 0    │ [F] 7    │
[F] 14   │ [F] 8    │ [F] 9    │ [F] 9    │ [F] 9    │
│ 20-29     │          │          │          │          │          │
        │          │          │          │          │
│ 30-39     │          │          │          │          │          │
        │          │          │          │          │

└──────────┴──────────┴──────────┴──────────┴──────────┴──────────┴
──────────┴──────────┴──────────┴──────────┴──────────┘
Member 2_01

┌──────────┬──────────┬──────────┬──────────┬──────────┬──────────┬
──────────┬──────────┬──────────┬──────────┬──────────┐
│ Range/IDX │ 0        │ 1        │ 2        │ 3        │ 4        │
5        │ 6        │ 7        │ 8        │ 9        │

├──────────┼──────────┼──────────┼──────────┼──────────┼──────────┼
──────────┼──────────┼──────────┼──────────┼──────────┤
│ 0-9       │ [S] 1    │ [S] 0    │ [S] 0    │ [S] 0    │ [S] 0    │
[S] 0    │ [S] 1    │ [F] 9    │ [F] 10   │ [F] 7    │
│ 10-19     │ [F] 9    │ [F] 4    │ [F] 6    │ [F] 6    │ [F] 4    │
[F] 6    │ [S] 0    │ [S] 0    │ [S] 0    │ [S] 0    │
│ 20-29     │ [S] 0    │ [S] 0    │ [S] 0    │ [F] 4    │ [F] 7    │
[F] 5    │ [F] 7    │ [F] 7    │ [F] 5    │ [F] 6    │
│ 30-39     │ [F] 8    │ [F] 7    │          │          │          │
        │          │          │          │          │

└──────────┴──────────┴──────────┴──────────┴──────────┴──────────┴
──────────┴──────────┴──────────┴──────────┴──────────┘
CPU Type: (F) - FWK, (S) - SND, (O) - Other

[Expert@SG-s01-01:0]#
```

Example 2 - 'cinfo interfaces'

```
[Expert@SG-s01-01:0]# cinfo interfaces
┌──────────────────────────────────── Interfaces
──────────────────────────────────────┐
│
                        │
│  Name        │ IP Address       │ Driver           │ State    │
Throughput │ Packet Rate  │
│
─────────────┼──────────────────┼──────────────────┼──────────┼────
──────┼──────────────┤
│  ethsBP1-01 │                  │ i40e             │ UP       │
171.9K     │ 97           │
│  ethsBP1-02 │                  │ i40e             │ UP       │
554.5K     │ 495          │
│  ethsBP1-03 │                  │ i40e             │ NO LINK  │ 0
       │ 0            │
│  ethsBP1-04 │                  │ i40e             │ NO LINK  │ 0
       │ 0            │
│  BPEth0     │                  │ bonding          │ UP       │
171.9K     │ 97           │
│  BPEth1     │                  │ bonding          │ UP       │
554.5K     │ 495          │
│  eth1-Mgmt1 │                  │ Pseudo Ethernet  │ UP       │
25.3K      │ 27           │
│  eth2-Mgmt1 │                  │ Pseudo Ethernet  │ UP       │
22.2K      │ 25           │
│  magg1      │ 10.33.25.66/24   │ bonding          │ UP       │
47.5K      │ 52           │
│  bond2      │                  │ bonding          │ NO LINK  │ 0
       │ 0            │
│  bond2.222  │ 10.33.222.66/24  │ vlan             │ UP       │ 0
       │ 0            │
│  bond2.223  │ 10.33.223.66/24  │ vlan             │ UP       │ 0
       │ 0            │
│  eth1-61    │                  │ Pseudo Ethernet  │ DOWN     │ 0
       │ 0            │
│  ethsBP2-01 │                  │ igb              │ NO LINK  │ 0
       │ 0            │
│  ethsBP2-02 │                  │ igb              │ NO LINK  │ 0
       │ 0            │
│  ethsBP2-03 │                  │ igb              │ NO LINK  │ 0
       │ 0            │
│  ethsBP2-04 │                  │ igb              │ NO LINK  │ 0
       │ 0            │
│
                        │
```

```
└──────────────────────────────────────────────────────────────────────────────
──────────────────────────┘

[Expert@SG-s01-01:0]#
```

cluster_site_admin

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Changes the administrative state (up or down) of the entire Site.

Use this command to initiate a manual failover from one Site to another Site.

Syntax

```
cluster_site_admin -h
```

```
cluster_site_admin -c <Site ID> {down | up}
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
<Site ID>	Specifies the Site ID: ■ `1` - Site #1 ■ `2` - Site #2

Related Commands

- *"set cluster sites-admin-state" on page 937*
- *"set cluster site-id <Site ID> admin-state" on page 939*
- *"set cluster members-admin-state" on page 933*
- *"cluster-cli" on page 863*
- *"g_clusterXL_admin" on page 896*
- *"insights" on page 903*
- *"asg stat" on page 829*
- *"asg monitor (on Security Groups)" on page 792*

config_verify

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Best Practice - Use one of these commands:

- *"insights" on page 903*
- *"hcp" on page 899*

Description

Verifies the configuration between the Security Group Members.

Syntax

```
config_verify
      -h
      -b <SGM IDs>
      -v
      -vs <VS ID>
      {-db_only | -xfer_only}
```

Parameters

Parameter	Description
-h	Shows the built-in help.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-v`	Shows verbose output.
`--vs <VS ID>`	Specifies the IDs of the Traditional VSX Virtual Systems. Applies to the Traditional Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.
`-db_only`	Examines only the main database file.
`-xfer_only`	Examines only the list of the required transferred files.

Examples

Example 1 - Success

```
[Expert@SG-s01-01:0]# config_verify -v
Performing DB verification... Passed
Performing xfer files verification... Passed

[Expert@SG-s01-01:0]#
```

Example 2 - Failure

```
[Expert@SG-s01-01:0]# config_verify -v
Performing DB verification... Passed
Performing xfer files verification... Failed!
+-----------------------------------------------------------------
--------+
|File: $FWDIR/conf/ip_port_feed.conf
       |
+-----------------------------------------------------------------
--------+
|File is identical on members:      |2_03 2_05
       |
+-----------------------------------+-------------------------
--------+
|File is identical on members:      |1_01 1_02 1_03 1_04 1_05 2_
01 2_02 |
|                                   |2_04
       |
+-----------------------------------+-------------------------
--------+

Comparing $FWDIR/conf/ip_port_feed.conf, members: 2_03,1_01
5c5
<       "If-Modified-Since" : "Sun, 20 Oct 2024 17:32:20 GMT"
---
>       "If-Modified-Since" : "Sun, 20 Oct 2024 17:28:22 GMT"

[Expert@SG-s01-01:0]#
```

core_dump_verifier

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Best Practice - Use one of these commands:

- *"insights" on page 903*
- *"hcp" on page 899*

Description

- Shows the core dump files - the user space and the kernel space.
- Deletes the existing core dump files.

Syntax

```
core_dump_verifier
      -h
      -a
      -c
      -k
      -v
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-a`	Includes the Security Group Members that are in the "DOWN" state.
`-c`	Deletes the existing core dump files from the user space.
`-k`	Deletes the existing core dump files from the kernel space.
`-v`	Shows the existing core dump files.

Examples

```
[Expert@SG-s01-01:0]# core_dump_verifier -a -v
Checking for process core dumps:
-*- 9 blades: 1_01 1_02 1_03 1_04 1_05 2_02 2_03 2_04 2_05 -*-
* No core dumps found *
-*- 1 blade: 2_01 -*-
2024-10-20 11:53:31.75505552
/var/log/dump/usermode/fwd.44371.core.gz

Checking for kernel core dumps:
-*- 10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 -
*-
* No core dumps found *

[Expert@SG-s01-01:0]#
```

cpha_vsx_util monitor

This command is supported only on these:

- Maestro Security Group in the Traditional VSX mode
- Scalable Chassis Security Group in the Traditional VSX mode

Notes:

- You must run this command in the Expert mode.
- This command does not apply to the VSNext mode.

Description

Starts and stops the monitoring of the Traditional VSX Virtual Systems.

The state of a Security Group Member is **not** affected by non-monitored Legacy Virtual Systems. For example, a non-monitored Legacy Virtual System in a problem state is ignored - the Security Group Member state does **not** change to DOWN.

Use Case

A Legacy 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 Legacy Virtual System is DOWN or does not have a Security Policy (for example, after you unload the local policy).

Syntax

```
cpha_vsx_util monitor
      {start | stop} <VS IDs>
      show
```

Parameters

Parameter	Description
`show`	Shows all non-monitored Legacy Virtual Systems.

Parameter	Description
`stop`	Stops the monitoring of the specified Legacy Virtual Systems. **Important** - When you stop the monitoring of a Legacy 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 Legacy Virtual Systems. By default, the monitoring is started for all configured Legacy .Virtual Systems
`<VS IDs>`	Applies to the Traditional Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.

Examples

```
[Expert@SG-s01-01:0]# cpha_vsx_util monitor show
1_01:

All VSs are monitored

1_02:

All VSs are monitored

1_03:

All VSs are monitored

[Expert@SG-s01-01:0]#
```

delete cluster

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description:

Deletes cluster settings.

Syntax:

```
delete cluster<ESC><ESC>
```

```
delete cluster
      configuration unique-ip site-id <ID of Standby Site>
interface <Name of Mgmt Interface>
      member method {hostname | serial-number | id} <VALUE>
[format json]
      site-id <Site ID>
            alert_threshold
            general
            module <Module>
            modules_amount
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: - `1` - Site #1 - `2` - Site #2 - `all` - All Sites

Parameter	Description
`delete cluster configuration unique-ip`	Removes a Management Interface from the UIPS configuration. For explanations, see: ■ For ElasticXL Cluster / Maestro: *"Configuring a Unique IP Address per Site (UIPS) in Maestro Dual Site" on page 208* ■ For Scalable Chassis: *"Configuring a Unique IP Address per Site (UIPS) in Dual Chassis" on page 389*
`delete cluster member method`	Removes a Security Appliance from the ElasticXL Cluster. See *"Working with ElasticXL Cluster" on page 30*.
`delete cluster site-id <Site ID>`	Specifies the Site ID, from which to remove the settings: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
`delete cluster site-id <Site ID> alert_threshold`	Removes the user-defined values for alert thresholds (restores the default values). Related commands: ■ *"show cluster alert_threshold" on page 957* ■ *"set cluster alert_threshold" on page 921*
`delete cluster site-id <Site ID> general`	Removes the general user-defined settings. Related commands: ■ *"set cluster site-id <Site ID> general" on page 943* ■ *"show cluster site-id <Site ID> general" on page 977*

Parameter	Description
`delete cluster site-id <Site ID> module <Module>`	Removes the specified module settings on Scalable Chassis: ■ `CMM` - Chassis Management Modules ■ `SSM1` - Security Switch Module #1 ■ `SSM2` - Security Switch Module #2 ■ `SSM3` - Security Switch Module #3 ■ `SSM4` - Security Switch Module #4 ■ `Mgmt` - Management Port Related commands: ■ *"set cluster site-id <Site ID> module" on page 944* ■ *"show cluster site-id <Site ID> module" on page 978*
`delete cluster site-id <Site ID> modules_amount`	Removes the user-defined number of modules on Scalable Chassis. Related commands: ■ *"set cluster site-id <Site ID> modules_amount" on page 946* ■ *"show cluster site-id <Site ID> modules_amount" on page 982*

delete smo

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Deletes settings related to the Single Management Object (SMO) on the Security Group.

Important - Do **not** use this command, unless Check Point Support or an Administration Guide explicitly tells you to do so.

Related Commands

- *"add smo" on page 824*
- *"show smo" on page 990*
- *"set smo" on page 954*

Syntax

```
delete smo
      security-group <SGM IDs>
      user-defined sync-file <File>
```

Parameters

Command	Description
`delete smo security-group <SGM IDs>`	Applies only to Scalable Chassis that has one Security Group. Deletes the specified Security Group Members from the Security Group. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`delete smo user-defined sync-file <File>`	Deletes the specified file for synchronization from the SMO. Press the TAB key to select the applicable file. The command deletes the specified files in this file: `/etc/xfer_file_list.user`

fw ctl get

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run the "`fw ctl get`" command in Gaia gClish.
- You must run the "`g_fw ctl get`" command the Expert mode to see the output for each Security Group Member.
  You can run the "`g_allc fw ctl get`" command the Expert mode to see the summarized output for all Security Group Members.

Description

Shows the current value for the specified kernel parameter.

For more information, see the *R82 Security Gateway Guide* > Chapter "**Working with Kernel Parameters** ".

Related Commands

- *"fw ctl set" on page 890*
- *"update_conf_file" on page 995*

Syntax

Syntax for Gaia gClish

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

Syntax for the Expert mode

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

Parameters

Parameter	Description
<Parameter Type>	Specifies the type of the parameter to query: ■ `int` - To query an integer parameter ■ `str` - To query a string parameter **Note** - You must enter the correct parameter type.
<Parameter Name>	Specifies the name of the parameter to query.

Examples

```
[Expert@SG-s01-01:0]# g_allc fw ctl get int fw_allow_simultaneous_ping
-*- 3 blades: 1_01 1_02 1_03 -*-
fw_allow_simultaneous_ping = 0

[Expert@SG-s01-01:0]#
```

fw ctl set

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run the "`fw ctl set`" command in Gaia gClish.
- You must run the "`g_fw ctl set`" command the Expert mode.

Best Practice - Use the *"update_conf_file" on page 995* command.

Description

Adds, updates, and removes parameters in the specified configuration file.

For more information, see the *R82 Security Gateway Guide* > Chapter "**Working with Kernel Parameters** ".

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

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 `$FWDIR/boot/modules/fwkern.conf` and `$PPKDIR/conf/simkern.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 (*"asg_cp2blades" on page 730*).

Related Commands

- *"fw ctl get" on page 888*
- *"update_conf_file" on page 995*

Syntax

Syntax for Gaia gClish

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

Syntax for the Expert mode

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

Parameters

Parameter	Description
<Parameter Type>	Specifies the type of the parameter to configure: ■ `int` - Configures an integer parameter ■ `str` - Configures a string parameter **Note** - You must enter the correct parameter type.
<Parameter Name>	Specifies the parameter name to configure.
<Parameter Value>	Specifies the parameter value to configure. For a string parameter, must be encloses in the double quote characters.

Examples

```
[Global] SG-s01-01> fw ctl set int fw_allow_simultaneous_ping 1
[Global] SG-s01-01>
```

g_all, g_allc, g_alls

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description

Runs the specified command on all Security Group Members and shows the requested output.

Syntax

```
{g_all | g_allc | g_alls}
      [-a] [-b <SGM IDs>] [--vs <VS ID>] [-l] [-r] <Expert mode
Command>
```

Parameters

Parameter	Description
`g_all`	Runs the specified command on each Security Group Member in the "UP" state. Shows the complete output from each Security Group Member in the "UP" state. The output is divided into sections for each Security Group Member.
`g_allc`	Collects the outputs from all Security Group Members (in the "UP" state) and: ■ If the outputs are identical, shows only one output. ■ If the outputs are different, shows only the different outputs.
`g_alls`	Shows the complete output from each Security Group Member in the "UP" state. The output shows the Security Group Member ID in the beginning of each line (this makes it easier to parse the output). This streaming output is suitable for commands that expect non-finite output, such as "`tcpdump`" of "`tail -f`".
No Parameters	Shows the outputs for all Security Group Members in the "UP" state.

Parameter	Description
`-a`	Includes the Security Group Members that are in the "DOWN" state.
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`--vs <VS ID>`	Specifies the IDs of the Traditional VSX Virtual Systems. Applies to the Traditional Virtual Systems as specified by the `<VS IDs>`. *<VS IDs>* can be: ■ No `<VS IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems This parameter is only applicable in a VSX environment.
`-l`	Shows the output only from the current Security Group Member, to which you are currently connected.
`-r`	Shows the output from Security Group Members, except the one to which you are currently connected.
`<Expert mode Command>`	Any Expert mode command (for example, `netstat`).

Examples

Example 1 - Viewing contents of a file

To demonstrate these commands, were created a test file on the Security Group Members:

- This file contains the same string on the Security Group Members 1_1 and 1_3.
- This file contains a different string on the Security Group Member 1_2.

```
[Expert@SG-s01-01:0]# g_all cat /var/log/test.txt
1_01:
Hello 123
1_02:
Hello 456
1_03:
Hello 123
[Expert@SG-s01-01:0]#

[Expert@SG-s01-01:0]# g_allc cat /var/log/test.txt
-*- 2 blades: 1_01 1_03 -*-
Hello 123
-*- 1 blade: 1_02 -*-
Hello 456

[Expert@SG-s01-01:0]#

[Expert@SG-s01-01:0]# g_alls cat /var/log/test.txt
[1_01]Hello 123
[1_02]Hello 456
[1_03]Hello 123
[Expert@SG-s01-01:0]#
```

Example 2 - Running a command that produces an output

```
[Expert@SG-s01-01:0]# g_all cp -v /var/log/test.txt{,_BKP}
1_01:
'/var/log/test.txt' -> '/var/log/test.txt_BKP'
1_02:
'/var/log/test.txt' -> '/var/log/test.txt_BKP'
1_03:
'/var/log/test.txt' -> '/var/log/test.txt_BKP'
[Expert@SG-s01-01:0]#

[Expert@SG-s01-01:0]# g_allc cp -v /var/log/test.txt{,_BKP}
-*- 3 blades: 1_01 1_02 1_03 -*-
'/var/log/test.txt' -> '/var/log/test.txt_BKP'

[Expert@SG-s01-01:0]#

[Expert@SG-s01-01:0]# g_alls cp -v /var/log/test.txt{,_BKP}
[1_01]'/var/log/test.txt' -> '/var/log/test.txt_BKP'
[1_02]'/var/log/test.txt' -> '/var/log/test.txt_BKP'
[1_03]'/var/log/test.txt' -> '/var/log/test.txt_BKP'
[Expert@SG-s01-01:0]#
```

g_clusterXL_admin

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Best Practices:

- In the Expert mode, use the *"cluster-cli" on page 863* command.
- In Gaia gClish, use the *"set cluster members-admin-state" on page 933* command.

Description

Changes the administrative state (up or down) of the specified Security Group Members.

Best Practices:

- Do **not** use this command in production environments without a good technical reason, because it can cause performance degradation (all connections will pass through the remaining Security Group Members).
- To ensure correct traffic failover within the Security Group, change the state of Security Group Members in the logical group one by one.

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 (see *"asg stat" on page 829*) 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 (see *"asg log" on page 775*):

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

Use Case

This command is useful for tests and debug.

You can install a Hotfix gradually on the Security Group Members while keeping the current connections.

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: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`up`	Changes the cluster state to UP on the specified Security Group Members.
`down`	Changes the cluster state to DOWN on the specified Security Group Members.
`-a`	Synchronizes accelerated connections to other Security Group Members.
`-r`	Runs this command on all `<SGM IDs>`, except the local Security Group Member, to which you are currently connected.

Examples

Example

```
[Expert@SG-s01-01:0]# 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@SG-s01-01:0]#
```

Related Commands

- *"cluster_site_admin" on page 874*
- *"set cluster members-admin-state" on page 933*
- *"set cluster sites-admin-state" on page 937*
- *"set cluster site-id <Site ID> admin-state" on page 939*
- *"insights" on page 903*
- *"asg stat" on page 829*
- *"asg monitor (on Security Groups)" on page 792*

hcp

This command is supported only on these:

- ElasticXL Cluster
- Maestro Orchestrator
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in the Expert mode.

Description:

HealthCheck Point (HCP) is a self-updatable suite of tools for:

- **Tests**: Assesses the health of your system
- **WTS (What's The Story)**: Provides a timeline of critical and informative events occurred on the system
- **Topology**: Visualize the Firewall topology

For more information and the complete syntax, see sk171436.

Syntax:

```
hcp --help
```

lightshot

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Maestro Orchestrator
- Scalable Chassis Security Group

Introduction to Gaia Lightshot

Each Regular Gaia Snapshot and each Scheduled Gaia Snapshot requires significant disk space (more than 12 gigabytes on a Security Gateway, more than 30 gigabytes on a VSX Gateway). It takes a long time to create these Gaia Snapshots.

Starting in R82, Gaia OS has an additional feature - Lightshot Snapshot. This snapshot type saves only the delta of the disk partition. As a result, it takes less disk space and less time to create each Lightshot Snapshot. The smaller the delta between the current state of the disk partition and the previous Lightshot Snapshot, the less disk space and less time are required.

Item	Lightshot Snapshot	Regular Gaia Snapshot, Scheduled Gaia Snapshot
Required disk space for each snapshot	Small.	Large.
Required time to create each snapshot	Short.	Long.
Required disk partition to store each snapshot	Uses one disk partition for all snapshots: `/mnt/lightshot`	Creates a dedicated disk partition for each snapshot.
Deleting an existing snapshot	You can delete snapshots only in the order they were created (from the latest to the earliest).	You can delete any snapshot in any order.
Exporting a new snapshot	Supported over the SSH protocol.	Supported over the FTP protocol and the SCP protocol.

Item	Lightshot Snapshot	Regular Gaia Snapshot, Scheduled Gaia Snapshot
Importing an existing snapshot	Supported over the SSH protocol.	Supported over the FTP protocol and the SCP protocol.
Scheduling a snapshot	Must use the Gaia Job Scheduler to run the Expert mode command "`lightshot`".	Supported directly in Gaia OS.

Automatic lightshot snapshot on Scalable Platform Security Groups

- The Gaia OS creates the first automatic lightshot snapshot immediately after installing the Gaia OS.
- The Gaia OS creates the second automatic lightshot snapshot immediately after the First Time Configuration Wizard.
- From this point, the Gaia OS creates automatic lightshot snapshot each night (at 03:00am).
- The Gaia OS keeps a total of five periodic lightshot snapshots and rotates them every day (the latest lightshot snapshot deletes the oldest lightshot snapshot).

Example:

```
[Expert@SG-s01-01:0]# lightshot show snapshots --verbose
┌──────────────────────────┬──────────────────────┬──────┬──────────────────────┐
│ Name                     │ Description          │ Size │ Date                 │
├──────────────────────────┼──────────────────────┼──────┼──────────────────────┤
│ fcd_Check_Point_Gaia_R82 │ None                 │ 8.0G │ 2024-10-15 09:05:10 │
│ Periodic_03_00_Oct_25_24 │ Periodic_Lightshot   │ 3.3G │ 2024-10-25 03:00:10 │
│ Periodic_03_00_Oct_26_24 │ Periodic_Lightshot   │ 141M │ 2024-10-26 03:00:11 │
│ Periodic_03_00_Oct_27_24 │ Periodic_Lightshot   │ 141M │ 2024-10-27 03:00:11 │
│ Periodic_03_00_Oct_28_24 │ Periodic_Lightshot   │ 141M │ 2024-10-28 03:00:11 │
│ Periodic_03_00_Oct_29_24 │ Periodic_Lightshot   │ 141M │ 2024-10-29 03:00:10 │
└──────────────────────────┴──────────────────────┴──────┴──────────────────────┘

[Expert@SG-s01-01:0]#
```

Syntax

See the *R82 Gaia Administration Guide* > Chapter "**Maintenance**" > Section "**Snapshot Management**" > Section "**Lightshot Snapshot**".

Note - Some Lightshot CLI features are different in Gaia gClish / Gaia Clish and in the Expert mode.

Syntax in the Expert mode:

```
lightshot -h
```

Syntax in Gaia gClish (on Security Groups) and in Gaia Clish (on Maestro Orchestrators):

```
add lightshot <Parameters>
```

```
set lightshot <Parameters>
```

```
show
      lightshot <Parameters>
      lightshot-partition <Parameters>
      lightshots <Parameters>
```

```
delete lightshot <Parameters>
```

insights

This command is supported only on these:

- ElasticXL Cluster
- Maestro Orchestrator
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You can run this command in Gaia gClish or in the Expert mode.
- In ElasticXL load sharing (with more than one Security Group Member per site), the Insights tool shows all traffic passing through the Single Management Object, including the traffic that the Single Management Object distributes to other Security Group Members.

Description:

Monitoring dashboard for Scalable Platforms (ElasticXL Cluster, Maestro, Scalable Chassis).

Requirement:

For the best view, configure the terminal application on your computer in this way:

- Terminal Type: `xterm`
- Font: `Consolas`
- Character Set (Encoding): `UTF-8 (Unicode)`
- Color Mode: `True Color`
- The terminal application window must show at least 190 columns and at least 25 rows

  Available options:

  - increase the size of the terminal application window
  - increase the resolution of your computer monitor

Syntax:

```
insights
      -h, --help
      --vs <VSID>
```

Parameters:

Parameter	Description
`-h`, `--help`	Shows the built-in help
`--vs` *<VSID>*	In the VSNext mode, runs the tool in the context of the specified Virtual Gateway

Tool interface:

- At the top, you can click different tabs:

Tab	Description
Overview	• Shows the overall information in these sections: ◦ **Hardware Overview** - shows the Type, Version, and Uptime ◦ **Access Policy** - click this section one time to see the information for all Cluster Members (Name and Installation Time) ◦ **Threat Prevention Policy** ◦ **Software Blades** - click this section one time to see the information for all Software Blades (Name, State, Entitlement, Expiration) ◦ **AI Detector** - click this section one time to see the detected issues (critical, error, warning, notice) and the next steps ◦ **CPU Usage** - click this section one time to see the information for all Cluster Members ◦ **Memory Usage** - click this section one time to see the information for all Cluster Members ◦ **Disk Space** - click this section one time to see the information for all Cluster Members ◦ **HCP Score** ◦ **Throughput** - click this section one time to see the information for all Cluster Members (for Data, Mgmt, and Sync) ◦ **Connection Rate** - shows the number of connections per seconds ◦ **Connections** - shows the number of concurrent connections ◦ **Packet Rate** - shows the number of packets per second ◦ **Drops** - click this section one time to see the information for all Cluster Members ◦ **Interfaces**- information about interfaces (Name, IP Address, Driver, State, Throughput, Packet Rate) ◦ **Site** - information about Sites and their Cluster Members Note - To close a popup window for a section, click outside its frame.

Tab	Description
Alerts	Shows issues detected by the HealthCheck Point (HCP) tests (see sk171436). 1. At the top, click the applicable tab: • Click **All** to see the HCP alerts for all Cluster Members (this is the default). • Click **<Site_ID>_<Member_ID>** to see the HCP alerts for the specific Cluster Member. 2. In the top right section **Severity**, you can click the severity levels to show the messages only with those severity levels. Note - The tool does not save this change and by default always shows messages with all severity levels.
HCP	Runs the HealthCheck Point (HCP) tests and shows their results (see sk171436): 1. At the top, click the applicable tab: • Click **All** to run the HCP tests on all Cluster Members (this is the default). • Click **<Site_ID>_<Member_ID>** to run the HCP tests on the specific Cluster Member. 2. In the top right corner, click **Run it**. 3. Wait for the tool to complete. 4. In the top right corner, click **Watch it**. Note - To close the **HCP Report** window, click outside its frame.
Tools	Runs various tools (for example, ConnView).

- At the bottom, there is a legend that shows the supported keys:

- **CTRL+C** - Quits the tool.
- **CTRL+S** - Saves a screenshot of the current screen.

  Explanation

  The tool saves the screenshots in the SVG format in the `/var/log/insights/` directory with these names:

  ```
  insights_<YYYY-MM-DD>T<HH_MM_SS_SSS>.svg
  ```

  Example:

  ```
  [Expert@EXL-1-s01-01:0]# cd /var/log/insights/
  [Expert@EXL-1-s01-01:0]# ls -l
  total 648
  -rw-rw---- 1 admin root 142885 Jun 24 15:22 insights_
  2024-06-24T15_22_35_691626.svg
  -rw-rw---- 1 admin root 183259 Jun 24 15:22 insights_
  2024-06-24T15_22_49_297335.svg
  -rw-rw---- 1 admin root 265023 Jun 24 15:22 insights_
  2024-06-24T15_22_56_089260.svg
  -rw-rw---- 1 admin root  65889 Jun 24 15:23 insights_
  2024-06-24T15_23_11_532412.svg
  [Expert@EXL-1-s01-01:0]#
  ```

- **CTRL+L** - Creates a Gaia Lightshot snapshot. This is useful for a later troubleshooting.

member

This command is supported only on these:

- ElasticXL Cluster
- Maestro Orchestrator
- Maestro Security Group
- Scalable Chassis Security Group

Note - Starting from R82, you can run this command in Gaia gClish or in the Expert mode.
(In R81.20 and lower, you must run this command in the Expert mode.)

Description

This commands moves you from the current shell to the shell on the specified target in the Scalable Platform.

See the explanations below in the corresponding sections.

Notes:

- To see the built-in help, run:
  `member -h`
- The command "`m`" is the alias for the command "`member`".
- After you run this command, the shell prompt changes to show the target ID.
- To exit from the target shell and return to the previous shell, run:
  `exit`

Syntax on ElasticXL Cluster

Explanation

In the ElasticXL Cluster, this commands moves you from the current shell in the Security Group to the shell in the specified Security Group Member:

```
member <ID of Site>_<ID of Security Group Member>
member <ID of Security Group Member>
```

Parameter	Description
<ID of Site>	Specifies the ID of the Site. This is mandatory in Dual Site. This is optional in Single Site.
ID of Security Group Member	Specifies the ID of the target Security Group Member in the target Security Group.

Example for the Security Group Member #2 on Site 2 in Dual Site:

```
member 2_2
```

Example for the Security Group Member #2 in Single Site:

```
m 2
```

Syntax on Maestro Orchestrator

Explanation

This commands moves you from the current shell on the Maestro Orchestrator to the shell on the specified Security Group Member.

```
member <ID of Security Group> <ID of Security Group Member>
```

Parameter	Description
<ID of Security Group>	Specifies the ID of the target Security Group.
ID of Security Group Member	Specifies the ID of the target Security Group Member in the target Security Group.

Example for the Security Group #1 and the Security Group Member #5:

```
member 1 5
```

```
m 1 5
```

Syntax on Maestro Security Group

Explanation

In the Maestro Security Group, this commands moves you:

- From the current shell in the Maestro Security Group to the shell in the specified Security Group Member.

```
member <ID of Site>_<ID of Security Group Member>
member <ID of Security Group Member>
```

- From the current shell in the Security Group Member to the shell on the specified Maestro Orchestrator on the current Site.

```
member {ssm1 | ssm2}
```

Parameter	Description
<ID of Site>	Specifies the ID of the Site. This is mandatory in Dual Site. This is optional in Single Site.
ID of Security Group Member	Specifies the ID of the target Security Group Member in the target Security Group.
ssm1 ssm2	Specifies the ID of the Maestro Orchestrator on the current Site: ■ ssm1 - Orchestrator #1 on the current Site ■ ssm2 - Orchestrator #2 on the current Site

Example for the Security Group Member #5 on Site 2 in Dual Site:

```
member 2_5
```

Example for the Security Group Member #5 in Single Site:

```
m 5
```

Example for the Orchestrator #2 on the current Site:

```
member ssm2
```

Syntax on Scalable Chassis

Explanation

On the Scalable Chassis, this commands moves you:

- From the current shell to the shell in the specified Security Group Member:

```
member <ID of Site>_<ID of Security Group Member>
member <ID of Security Group Member>
```

- From the current shell to the shell in the specified Security Switch Module (SSM):

```
member {ssm1 | ssm2 | ssm3 | ssm4}
```

- From the current shell to the shell in the Chassis Management Module (CMM):

```
member cmm
```

Parameter	Description
<ID of Site>	Specifies the ID of the Site. This is mandatory in Dual Site. This is optional in Single Site.
ID of Security Group Member	Specifies the ID of the target Security Group Member in the target Security Group.

Parameter	Description

`ssm1`
`ssm2`
`ssm3`
`ssm4`
	Specifies the ID of the SSM on the current Scalable Chassis:
	■ `ssm1` - SSM #1 on the current Scalable Chassis
	■ `ssm2` - SSM #2 on the current Scalable Chassis
	■ `ssm3` - SSM #3 on the current Scalable Chassis
	■ `ssm4` - SSM #4 on the current Scalable Chassis

`cmm`	Specifies the context of the CMM.

For information about SSM and CMM, see the *Scalable Chassis Getting Started Guide*.

Example for the Security Group Member #5 on Site 2 in Dual Site:

```
member 2_5
```

Example for the Security Group Member #5 in Single Site:

```
m 5
```

Example for the SSM #2 on the current Scalable Chassis:

```
member ssm2
```

Related Commands

Explanation

To see the information about Security Group Members, use any of these commands:

Shell	Command	Reference
Expert mode Gaia gClish	`asg stat -v`	*"asg stat" on page 829*
Expert mode	`insights`	*"insights" on page 903*
Expert mode	`cluster-cli show info overview`	*"cluster-cli" on page 863*
Gaia gClish	`show cluster info overview`	*"show cluster info" on page 967*
Expert mode	`orch_stat -t`	*"orch_stat" on page 1017*

reboot

This command is supported on all these:

- ElasticXL Cluster
- Maestro Orchestrator
- Maestro Security Group
- Scalable Chassis Security Group

Description

This command performs the software reboot.

Related Commands

- *"cluster-cli" on page 863*
- *"set cluster members-reboot" on page 935*
- *"asg_reboot" on page 811*

Syntax in Gaia gClish or the Expert mode

```
reboot
```

Important - You can run this command in Gaia Clish or in the Expert mode only on a Maestro Orchestrator.

Syntax in Gaia gClish

```
reboot
      -h
      -b <SGM IDs> [-a]
```

Important - You must run this command in Gaia gClish on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Parameters in Gaia gClish

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows the brief command usage.
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. By default, applies to all Security Group Members. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-a`	Runs the command also on Security Group Members in the Administrative "DOWN" state.

Example 1 - Reboot only specific Security Group Members

```
[Global] SG-s01-01> reboot -b 1_02,1_03
You are about to perform reboot on members: 1_02,1_03
It might cause performance hit for a period of time.

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

Reboot requires auditing
Enter your full name: John Doe
Enter reason for reboot [Maintenance]: Troubleshooting
WARNING: Reboot on members: 1_02,1_03, User: John Doe, Reason:
Troubleshooting
[Global] SG-s01-01>
```

Example 2 - Reboot all Security Group Members, including those in the state "DOWN"

```
[Global] SG-s01-01> reboot -b all -a
You are about to perform reboot on members: 1_01,1_02,1_03,2_01,2_
02,2_03
It might cause performance hit for a period of time.

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

Reboot requires auditing
Enter your full name: John Doe
Enter reason for reboot [Maintenance]: Troubleshooting
WARNING: Reboot on members: 1_01,1_02,1_03,2_01,2_02,2_03, User:
John Doe, Reason: Troubleshooting
[Global] SG-s01-01>
```

set cluster

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings (see the corresponding pages).

Syntax

```
set cluster<ESC><ESC>
```

set cluster alert_threshold

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description:

Configures cluster settings - values for alert thresholds.

Related Commands

- *"show cluster alert_threshold" on page 957*
- *"delete cluster" on page 883*

Syntax:

```
set cluster alert_threshold<ESC><ESC>
```

```
set cluster alert_threshold
      concurr_conn_threshold_high <Value>
      concurr_conn_threshold_low_ratio <Value>
      concurr_conn_total_threshold_high <Value>
      concurr_conn_total_threshold_low_ratio <Value>
      conn_rate_threshold_high <Value>
      conn_rate_threshold_low_ratio <Value>
      conn_rate_total_threshold_high <Value>
      conn_rate_total_threshold_low_ratio <Value>
      cpu_load_threshold_perc_high <Value>
      cpu_load_threshold_perc_low_ratio <Value>
      hd_util_threshold_perc_high <Value>
      hd_util_threshold_perc_low_ratio <Value>
      mem_util_threshold_perc_high <Value>
      mem_util_threshold_perc_low_ratio <Value>
      packet_rate_threshold_high <Value>
      packet_rate_threshold_low_ratio <Value>
      packet_rate_total_threshold_high <Value>
      packet_rate_total_threshold_low_ratio <Value>
      throughput_threshold_high <Value>
      throughput_threshold_low_ratio <Value>
      throughput_total_threshold_high <Value>
      throughput_total_threshold_low_ratio <Value>
```

Parameters

Parameter	Description
`concurr_conn_threshold_high <Value>`	Configures the high threshold for concurrent connections, for each CoreXL Firewall instance. Default: 2,000,000
`concurr_conn_threshold_low_ratio <Value>`	Configures the low threshold for concurrent connections, as percentage from the high threshold. Default: 80.
`concurr_conn_total_threshold_high <Value>`	Configures the high threshold for concurrent connections. Accumulative for all CoreXL Firewall instances. Default: 20,000,000.

Parameter	Description
`concurr_conn_total_threshold_low_ratio <Value>`	Configures the low threshold for concurrent connections, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances Default: 80.
`conn_rate_threshold_high <Value>`	Configures the high threshold for connection rate (conn/sec), for each CoreXL Firewall instance. Default: 30000.
`conn_rate_threshold_low_ratio <Value>`	Configures the low threshold for connection rate, as percentage from the high threshold. Default: 80.
`conn_rate_total_threshold_high <Value>`	Configures the high threshold for connection rate (conn/sec). Accumulative for all CoreXL Firewall instances. Default: 300,000.
`conn_rate_total_threshold_low_ratio <Value>`	Configures the low threshold for connection rate, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances. Default: 80.
`cpu_load_threshold_perc_high <Value>`	Configures the high threshold for CPU load (%). Default: 75.
`cpu_load_threshold_perc_low_ratio <Value>`	Configures the low threshold for CPU load, as percentage from the high threshold. Default: 80.
`hd_util_threshold_perc_high <Value>`	Configures the high threshold for hard drive utilization (%). Default: 80.
`hd_util_threshold_perc_low_ratio <Value>`	Configures the low threshold for hard drive utilization, as percentage from the high threshold. Default: 80.
`mem_util_threshold_perc_high <Value>`	Configures the high threshold for memory utilization (%). Default: 50.
`mem_util_threshold_perc_low_ratio <Value>`	Configures the low threshold for memory utilization, as percentage from the high threshold. Default: 80.

Parameter	Description
`packet_rate_threshold_high <Value>`	Configures the high threshold for packet rate (packets/sec), for each CoreXL Firewall instance. Default: 1,000,000.
`packet_rate_threshold_low_ratio <Value>`	Configures the low threshold for packet rate, as percentage from the high threshold. Default: 80.
`packet_rate_total_threshold_high <Value>`	Configures the high threshold for packet rate (packets/sec). Accumulative for all CoreXL Firewall instances. Default: 10,000,000.
`packet_rate_total_threshold_low_ratio <Value>`	Configures the low threshold for packet rate, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances. Default: 80.
`throughput_threshold_high <Value>`	Configures the high threshold for throughput (bits/sec), for each CoreXL Firewall instance. Default: 3,000,000,000.
`throughput_threshold_low_ratio <Value>`	Configures the low threshold for throughput, as percentage from the high threshold. Default: 80.
`throughput_total_threshold_high <Value>`	Configures the high threshold for throughput (bits/sec). Accumulative for all CoreXL Firewall instances. Default: 30,000,000,000.
`throughput_total_threshold_low_ratio <Value>`	Configures the low threshold for throughput, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances. Default: 80.

set cluster configuration high-availability

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - High Availability values.

Related Commands

- *"show cluster configuration high-availability" on page 960*

Syntax

```
set cluster configuration high-availability<ESC><ESC>
```

```
set cluster configuration high-availability
      bond <Name of Bond> min_slaves <1-8>
      down_on_first_join {0 | 1}
      factors
            member <0-1000>
            pnote pingable_hosts <0-1000>
            port bond <0-1000>
            port mgmt <0-1000>
            port other <0-1000>
            port standard <0-1000>
            sensor cmm <0-1000>
            sensor fans <0-1000>
            sensor power_supplies <0-1000>
            sensor ssm <0-1000>
      failover <0-1000>
      freeze_interval {0 | <1-1000>}
      mgmt-monitoring {on | off}
      mode {0 | 1 | 2 | 3}
      port <Name of Port> priority {1 | 2}
      vs site_priority "<ID of Primary Site> <ID of Secondary
Site>"
```

Explanation for Grade Factors

In a Dual Site environment, the Site with the higher grade becomes the Active Site and handles traffic.

The grade for each component is calculated based on this formula:

```
(Unit Weight) x (Number of Components in the State "UP")
```

To see the weight of each component, run this command in Gaia gClish and refer to the column "`Weight`" (see *"asg stat" on page 829*):

```
asg stat -v
```

For additional information, see:

- For Maestro - *"Configuring Security Group High Availability in Maestro" on page 255*.
- For Scalable Chassis - *"Configuring Scalable Chassis High Availability" on page 374*.

Parameters

Parameter	Description
`bond <Name of Bond> min_slaves <1-8>`	Configures the minimum number of subordinate interfaces in the "UP" state in the specified bond interface. If the number of subordinate interfaces in the "UP" state is lower than the configured threshold, then the cluster state of this bond interface changes to "DOWN".
`down_on_first_join {0 | 1}`	Configures whether a Security Group Member must remain in the Administratively Down state when it joins the Security Group. ■ 0 - Does **not** enable the administratively DOWN state for the first join. ■ 1 - Enables the administratively DOWN state for the first join. See: ■ For ElasticXL Cluster and Maestro, see *"Setting the Administratively DOWN State on First Join" on page 571*. ■ For Scalable Chassis, see *"Setting the Administratively DOWN State on First Join in Dual Chassis" on page 387*.
`factors member <0-1000>`	Configures the Grade factor for the component "Security Group Member".

Parameter	Description
`factors pnote pingable_hosts <0-1000>`	Configures the Grade factor for the component "Critical Device 'Pingable Hosts'".
`factors port bond <0-1000>`	Configures the Grade factor for the component "Bond Interfaces".
`factors port mgmt <0-1000>`	Configures the Grade factor for the component "Management Ports".
`factors port other <0-1000>`	Configures the High Grade factor for the component "Ports".
`factors port standard <0-1000>`	Configures the Standard Grade factor for the component "Ports".
`factors sensor cmm <0-1000>`	Configures the Grade factor for the component "CMMs" (only on Scalable Chassis).
`factors sensor fans <0-1000>`	Configures the Grade factor for the component "Fans" (only on Scalable Chassis).
`factors sensor power_supplies <0-1000>`	Configures the Grade factor for the component "Power Supply Units" (only on Scalable Chassis).
`factors sensor ssm <0-1000>`	Configures the Grade factor for the component "SSMs" (only on Scalable Chassis). This factor applies to all SSMs.
`failover <0-1000>`	Configures the minimum quality grade differential that causes a failover.

Parameter	Description
`freeze_interval {0 | <1-1000>}`	A Standby Site cannot failover a second time until the specified failover freeze interval expires. If the Standby Site grade changes to a value greater than the minimum quality grade gap for a failover, the Standby Site fails over and becomes a new Active Site. The failover does not start until the freeze interval expires. This confirms that the Standby Site quality grade is stable, before it becomes a new Active Site. The default failover freeze interval is: ■ 30 seconds for the "Active Up" mode ("`set cluster configuration high-availability mode 0`"). ■ 150 seconds for the "Primary Up" mode ("`set cluster configuration high-availability mode 1`"). ■ 150 seconds for the "VSLS" mode ("`set cluster configuration high-availability mode 3`"). Valid freeze time values: ■ Value 0 - Disables this threshold. ■ Values 1-1000 - Specifies the freeze time in seconds. If this Security Group is configured to work in the "VSLS" mode or in the "Primary Up" mode, then you must enter the value that is 5 times smaller that the required freeze time. Example: If the freeze time must be 250 seconds, you must enter the value 50.
`mgmt-monitoring {on | off}`	Configures whether to monitoring the Management Ports: ■ `on` - Enables the monitoring of the Management Ports. • The monitored management ports are included in the Standby Site grade mechanism, according to the predefined factors. • The output of the "`asg stat -v`" command shows the Management ports. • The "`show interfaces`" command in Gaia gClish shows the link state of management interfaces based on this feature mechanism. ■ `off` - Disables the monitoring of the Management Ports (this is the default).

Parameter	Description
`mode {0 | 1 | 2 | 3}`	Configures the Dual Site mode: ■ `0` - No primary Site ("Active Up" Mode) ■ `1` - "Primary Up" Mode ■ `2` - "Active Active" Mode ■ `3` - Traditional VSX Virtual System Load Sharing (VSLS) Mode

`port <Name of Port> priority {1 | 2}`	Configures the Priority Level for the specified port:
	■ `1` - Standard.
	■ `2` - Other.
	Use the "`set cluster configuration high-availability port ... priority ...`" command together with the "`set cluster configuration high-availability factors port ...`" command:
	1. Set the port grade as standard or high.
	For example, to set the standard grade at 50, run:
	`set cluster configuration high-availability factors port standard 50`
	2. Set the port to high grade or standard grade.
	For example, to assign the standard port grade to `eth1-01`, run:
	`set cluster configuration high-availability port eth1-01 priority 1`

`vs site_priority "<ID of Primary Site> <ID of Secondary Site>"`	Configures the priority for each Site for the current Traditional VSX Virtual System. You must run this command in the context of the applicable Virtual System. Example - Configuration of Site 2 to be the Primary and Site 1 to be the Secondary for the Virtual System 4: 1. `set virtual-system 4` 2. `set cluster high-availability vs site_priority "2 1"`

set cluster configuration image

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - SMO Image Cloning in the Security Group.

Related Commands

- *"show cluster configuration image" on page 964*

Syntax

```
set cluster configuration image<ESC><ESC>
      auto-clone state {on | off}
      md5sum
```

Parameters

Parameter	Description
`auto-clone state {on | off}`	Enables (`on`) or disables (`off`) the SMO Image Cloning in the Security Group.
`md5sum`	Calculates the MD5 sum of the SMO Image.

set cluster configuration unique-ip

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - Unique IP Address per Site (UIPS).

For explanation, see:

- For ElasticXL Cluster / Maestro:

  "Configuring a Unique IP Address per Site (UIPS) in Maestro Dual Site" on page 208

- For Scalable Chassis:

  "Configuring a Unique IP Address per Site (UIPS) in Dual Chassis" on page 389

Related Commands

- *"show cluster configuration unique-ip" on page 965*
- *"delete cluster" on page 883*

Syntax

```
set cluster configuration unique-ip<ESC><ESC>
```

```
set cluster configuration unique-ip site-id <ID of Standby Site>
      apply_unique_config
      interface <Name of Mgmt Interface> ipv4-address <IPv4
Address> mask-length <Length of Subnet Mask>
```

Parameters

Parameter	Description
<ID of Standby Site>	Specifies the ID of the Standby Site / Standby Chassis: Valid values: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
<Name of Mgmt Interface>	Specifies the name of the Management Interface that is assigned to the Security Group. For example, `eth1-Mgmt1`.
<IPv4 Address>	Specifies the alias IPv4 address on the same network as one of the Security Group Members' interfaces.
<Length of Subnet Mask>	Specifies the length of the IPv4 subnet mask.

set cluster members-admin-state

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run this command in Gaia gClish.
- For the Expert mode, see *"cluster-cli" on page 863*.

Description

Configures cluster settings - administrative state (up or down) of the specified Security Group Members.

Best Practice - Do **not** use this command in production environments without a good technical reason, because it can cause performance degradation (all connections will pass through the remaining Security Group Members).

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 (see *"asg stat" on page 829*) 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.

Use Case

This command is useful for tests and debug.

You can install a Hotfix gradually on the Security Group Members while keeping the current connections.

Syntax

```
set cluster members-admin-state<ESC><ESC>
      ids <SGM ID> {up | down}
      local {up | down}
      remote {up | down}
```

Parameters

Parameter	Description
`ids <SGM ID> {up | down}`	Configures the administrative state (up or down) for the specified Security Group Members. `<SGM IDs>` can be: ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`)
`local {up | down}`	Configures the administrative state (up or down) of all Security Group Members on the local Site (to which you are connected).
`remote {up | down}`	Configures the administrative state (up or down) of all Security Group Members on the remote Site.

Related Commands

- *"show cluster info" on page 967*
- *"set cluster sites-admin-state" on page 937*
- *"set cluster site-id <Site ID> admin-state" on page 939*
- *"cluster_site_admin" on page 874*
- *"cluster-cli" on page 863*
- *"g_clusterXL_admin" on page 896*
- *"insights" on page 903*
- *"asg stat" on page 829*
- *"asg monitor (on Security Groups)" on page 792*

set cluster members-reboot

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Reboots all Security Group Members on the specified Site.

Syntax

```
set cluster members-reboot<ESC><ESC>
```

```
set cluster members-reboot
      ids <SGM IDs>
      local
      remote
```

Parameters

Parameter	Description
<SGM IDs>	Specifies the Security Group Members. *<SGM IDs>* can be: ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`)
`local`	Reboots all Security Group Members on the local Site, to which you are currently connected.
`remote`	Reboots all Security Group Members on the remote Site.

Related Commands

- *"cluster-cli" on page 863*
- *"asg_reboot" on page 811*

set cluster sites-admin-state

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run this command in Gaia gClish.
- For the Expert mode, see *"cluster-cli" on page 863*.

Description

Configures cluster settings - administrative state (up or down) of the entire Site.

Note - This command does **not** change the administrative state of the Security Group Members.

Best Practice - Do **not** use this command in production environments without a good technical reason, because it can cause performance degradation (all connections will pass through the remaining Site).

Use Case

This command is useful for tests and debug.

You can install a Hotfix gradually on the Security Group Members while keeping the current connections.

Syntax

```
set cluster sites-admin-state<ESC><ESC>
      id <Site ID> {down | up}
      local {down | up}
      remote {down | up}
```

Parameters

Parameter	Description
`ids <Site ID> {up | down}`	Configures the administrative state (up or down) of the specified Site: ■ `1` - Applies to Site #1 ■ `2` - Applies to Site #2
`local {up | down}`	Configures the administrative state (up or down) of the local Site (to which you are connected).
`remote {up | down}`	Configures the administrative state (up or down) of the remote Site.

Related Commands

- *"show cluster info" on page 967*
- *"set cluster members-admin-state" on page 933*
- *"set cluster site-id <Site ID> admin-state" on page 939*
- *"cluster_site_admin" on page 874*
- *"cluster-cli" on page 863*
- *"g_clusterXL_admin" on page 896*
- *"insights" on page 903*
- *"asg stat" on page 829*
- *"asg monitor (on Security Groups)" on page 792*

set cluster site-id <Site ID> admin-state

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run this command in Gaia gClish.
- For the Expert mode, see *"cluster-cli" on page 863*.

Description

Configures cluster settings - administrative state (up or down) of the entire Site.

Note - This command does **not** change the administrative state of the Security Group Members.

Best Practice - Do **not** use this command in production environments without a good technical reason, because it can cause performance degradation (all connections will pass through the remaining Site).

Use Case

This command is useful for tests and debug.

You can install a Hotfix gradually on the Security Group Members while keeping the current connections.

Syntax

```
set cluster site-id <Site ID> admin-state {up | down} [force]
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: - `1` - Site #1 - `2` - Site #2 The value "`all`" is not supported for this command.

Related Commands

- *"show cluster info" on page 967*
- *"set cluster sites-admin-state" on page 937*
- *"set cluster members-admin-state" on page 933*
- *"cluster_site_admin" on page 874*
- *"cluster-cli" on page 863*
- *"g_clusterXL_admin" on page 896*
- *"insights" on page 903*
- *"asg stat" on page 829*
- *"asg monitor (on Security Groups)" on page 792*

set cluster site-id <Site ID> alert_threshold

This command is supported only on:

- Scalable Chassis

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - thresholds for hardware alerts.

Syntax

```
set cluster site-id <Site ID> alert_threshold<ESC><ESC>
```

```
set cluster site-id <Site ID> alert_threshold
      cpus_temperature_threshold_high <1-100 °C>
      cpus_temperature_threshold_low <1-100 °C>
      fans_threshold_high <1-15>
      fans_threshold_low <1-15>
      power_consumption_threshold_perc_high <1-100 %>
      power_consumption_threshold_perc_low <1-100 %>
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: ■ 1 - Site #1 ■ 2 - Site #2 ■ all - All Sites
cpus_temperature_threshold_high	Configures the high threshold for CPU temperature (°C). Default: 95.
cpus_temperature_threshold_low	Configures the low threshold for CPU temperature (°C). Default: 60.
fans_threshold_high	Configures the high threshold for fans speed. Default: 11.
fans_threshold_low	Configures the low threshold for fans speed. Default: 9.
power_consumption_threshold_perc_high	Configures the high threshold for power consumption (%). Default: 90.
power_consumption_threshold_perc_low	Configures the low threshold for power consumption (%). Default: 80.

Related Commands

- *"show cluster site-id <ID> alert_threshold" on page 975*
- *"set cluster alert_threshold" on page 921*
- *"show cluster alert_threshold" on page 957*
- *"delete cluster" on page 883*

set cluster site-id <Site ID> general

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - general user-defined settings.

Syntax

```
set cluster site-id <Site ID> general<ESC><ESC>
```

```
set cluster site-id <Site ID> general
      snmp_retries <Number of Retires>
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
`snmp_retries` *<Number of Retires>*	Configures the number of retries before timeout. Default: 3.

Related Commands

- *"show cluster site-id <Site ID> general" on page 977*
- *"delete cluster" on page 883*

set cluster site-id <Site ID> module

This command is supported only on:

- Scalable Chassis

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - hardware components on Scalable Chassis.

Syntax

```
set cluster site-id <Site ID> module<ESC><ESC>
```

```
set cluster site-id <Site ID> module <Module>
      ip <IP Address>
      ports_amount <Number>
      secondary_ip <IP Address>
      snmp_auth <Authentication Method>
      status {active | down}
      username <Username>
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
<Module>	Specifies the hardware module: ■ `CMM` - CMMs ■ `SSM1` - SSM #1 ■ `SSM2` - SSM #2 ■ `SSM3` - SSM #3 ■ `SSM4` - SSM #4 ■ `Mgmt` - Management Ports
`ip` *<IP Address>*	Configures the primary IP address. Applies only to the SSM modules.

Parameter	Description
`ports_amount <Number>`	Configures the number of ports. Applies only to the SSM and Management Ports modules.
`secondary_ip <IP Address>`	Configures the secondary IP address. Applies only to the CMM modules.
`snmp_auth <Authentication Method>`	Configures the SNMP Authentication method: ■ `MD5` (this is the default) ■ `SHA1` ■ `none` Applies only to the SSM and Management Ports modules.
`status {active | down}`	Configures the status. Applies only to the SSM and Management Ports modules.
`username <Username>`	Configures the internal username. Default: `asg1` Applies only to the SSM and Management Ports modules.

Related Commands

- *"show cluster site-id <Site ID> module" on page 978*
- *"show cluster site-id <Site ID> modules_amount" on page 982*
- *"asg hw_monitor" on page 1051*
- *"delete cluster" on page 883*

set cluster site-id <Site ID> modules_amount

This command is supported only on:

- Scalable Chassis

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - the required number of hardware components.

Syntax

```
set cluster site-id <Site ID> modules_amount<ESC><ESC>
```

```
set cluster site-id <Site ID> modules_amount
      cmm <1-2>
      fans <1-6>
      power_units <1-6>
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: - `1` - Site #1 - `2` - Site #2 - `all` - All Sites
`cmm`	Configures the required number of Chassis Management Modules (CMMs).
`fans`	Configures the required number of Fans.
`power_units`	Configures the required number of Power Supply Units (PSU).

Related Commands

- *"show cluster site-id <Site ID> modules_amount" on page 982*
- *"set cluster site-id <Site ID> alert_threshold" on page 941*
- *"show cluster site-id <ID> alert_threshold" on page 975*
- *"asg hw_monitor" on page 1051*
- *"delete cluster" on page 883*

set cluster vsls

This command is supported only on these:

- Maestro Security Group in the Traditional VSX mode
- Scalable Chassis Security Group in the Traditional VSX mode

Note - You must run this command in Gaia gClish.

Description

Configures cluster settings - in the Traditional VSX mode, configures the Virtual System Load Sharing (VSLS) settings.

Syntax

```
set cluster vsls<ESC><ESC>
```

```
set cluster vsls
      member_ratio <1-100 %>
      system
            mgmt_monitoring {VS0_only | all_VSs}
            primary_site {0 | 1 | 2}
```

Parameters

Parameter	Description
`member_ratio <1-100 %>`	Configures the VSLS cluster member ratio.
`system mgmt_monitoring {VS0_only | all_VSs}`	Configures which Virtual Systems monitor the Management Port link state: ■ `VS0_only` Only VS0 monitors the link state of the Management Port. Failover occurs only for VS0 and the SMO. ■ `all_VSs` All Virtual Systems decide their state based on link state of the Management Port. Failover occurs for all Virtual Systems.
`system primary_site {0 | 1 | 2}`	Configures the VSLS Primary Site: ■ `0` - The Security Group decides automatically, based on the Virtual System ID. ■ `1` - Site 1 is the primary Site. ■ `2` - Site 2 is the primary Site.

Related Commands

- *"show cluster vsls" on page 986*
- *"set cluster configuration high-availability" on page 925*
- *"show cluster configuration high-availability" on page 960*

set distribution

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Configures the settings for the Distribution Mode.

See *"Working with the Distribution Mode" on page 554*.

Related Commands

- *"show distribution" on page 988*

Syntax

```
set distribution
      configuration {auto-topology | manual-general} ip-version
{ipv4 | ipv6 | all} ip-mask <Mask>
      interface <Name of Interface> configuration {user | network
| policy}
      l4-mode {disabled | enabled}
      matrix-max-size {1k | 2k | 4k | 8k | 16k}
      spi mode {on | off}
```

Commands

Command	Description
`set distribution configuration`	Configures the Distribution Mode settings.
`set distribution interface`	Configures the Interface Distribution Mode.
`set distribution l4-mode`	Configures the Layer 4 Distribution Mode.
`set distribution matrix-max-size`	Configures the maximum size for the Distribution Mode Matrix.
`set distribution spi`	Enables or disables the SPI Distribution Mode.

Parameters

Parameters for 'set distribution configuration'

Parameter	Description
`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.

`ip-mask <Mask>`	Must be the same as the distribution matrix size.
	Must be specified in the Hex format.
	Follow these steps:
	1. Examine the distribution matrix size:
	`show distribution verification verbose`
	Examine the `Matrix Size` line.
	Example:
	`... Matrix Size 512 ...`
	2. Exit from the Gaia gClish to the Expert mode.
	3. Convert the matrix size from the decimal to the hexadecimal format:
	`printf '%x\n' <Matrix Size>`
	Example:
	`[Expert@SG-s01-01:0]# printf '%x\n' 512 200 [Expert@SG-s01-01:0]#`
	4. Go to the Gaia gClish:
	`gclish`
	5. Configure the distribution mode with the required mask:
	`set distribution ... ip-mask <Matrix Size in HEX>`
	Example:
	`set distribution ... ip-mask 200`

Parameters for 'set distribution interface'

Parameters

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

set smo

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Configures settings related to the Single Management Object (SMO) on the Security Group.

Important - Do **not** use this command, unless Check Point Support or an Administration Guide explicitly tells you to do so.

Related Commands

- *"add smo" on page 824*
- *"show smo" on page 990*
- *"delete smo" on page 886*

Syntax

```
set smo
      audit-log expert-mode {on | off}
      security-group
            sgm-weight
                  member-id <SGM IDs> weight {default | <0-512>}
                  apply
            site-amount {1 | 2}
      user-defined
            sync-file apply
```

Commands

Command	Description
`set smo audit-log expert-mode {on | off}`	Enables or disables the audit logs for SMO operations in the Expert mode.
`set smo security-group sgm-weight`	On a Maestro Security Group with different Security Appliances, configures weights for Security Group Members to balance the traffic proportionally. See *"Configuring Weights for Security Group Members in Maestro" on page 174*.
`set smo security-group site-amount {1 | 2}`	Configures the number of Sites in a Security Group.
`set smo user-defined sync-file apply`	Enables the synchronization of user-defined files from the SMO. You must configure the required files with the "*"add smo" on page 824*" command.

show cluster

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows cluster configuration (see the corresponding pages).

Syntax

```
show cluster<ESC><ESC>
```

show cluster alert_threshold

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows cluster configuration - values for alert thresholds.

Related Commands

- *"set cluster alert_threshold" on page 921*
- *"delete cluster" on page 883*

Syntax

```
show cluster alert_threshold<ESC><ESC>
```

Parameters

Parameter	Description
`concurr_conn_threshold_high`	Shows the high threshold for concurrent connections, for each CoreXL Firewall instance.
`concurr_conn_threshold_low_ratio`	Shows the low threshold for concurrent connections, as percentage from the high threshold.
`concurr_conn_total_threshold_high`	Shows the high threshold for concurrent connections. Accumulative for all CoreXL Firewall instances.
`concurr_conn_total_threshold_low_ratio`	Shows the low threshold for concurrent connections, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances
`conn_rate_threshold_high`	Shows the high threshold for connection rate (conn/sec), for each CoreXL Firewall instance.

Parameter	Description
`conn_rate_threshold_low_ratio`	Shows the low threshold for connection rate, as percentage from the high threshold.
`conn_rate_total_threshold_high`	Shows the high threshold for connection rate (conn/sec). Accumulative for all CoreXL Firewall instances.
`conn_rate_total_threshold_low_ratio`	Shows the low threshold for connection rate, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances.
`cpu_load_threshold_perc_high`	Shows the high threshold for CPU load (%).
`cpu_load_threshold_perc_low_ratio`	Shows the low threshold for CPU load, as percentage from the high threshold.
`hd_util_threshold_perc_high`	Shows the high threshold for hard drive utilization (%).
`hd_util_threshold_perc_low_ratio`	Shows the low threshold for hard drive utilization, as percentage from the high threshold.
`mem_util_threshold_perc_high`	Shows the high threshold for memory utilization (%).
`mem_util_threshold_perc_low_ratio`	Shows the low threshold for memory utilization, as percentage from the high threshold.
`packet_rate_threshold_high`	Shows the high threshold for packet rate (packets/sec), for each CoreXL Firewall instance.
`packet_rate_threshold_low_ratio`	Shows the low threshold for packet rate, as percentage from the high threshold.
`packet_rate_total_threshold_high`	Shows the high threshold for packet rate (packets/sec). Accumulative for all CoreXL Firewall instances.
`packet_rate_total_threshold_low_ratio`	Shows the low threshold for packet rate, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances.
`throughput_threshold_high`	Shows the high threshold for throughput (bps), for each CoreXL Firewall instance.
`throughput_threshold_low_ratio`	Shows the low threshold for throughput, as percentage from the high threshold.

Parameter	Description
`throughput_total_ threshold_high`	Shows the high threshold for throughput (bits/sec). Accumulative for all CoreXL Firewall instances.
`throughput_total_ threshold_low_ratio`	Shows the low threshold for throughput, as percentage from the high threshold. Accumulative for all CoreXL Firewall instances.

show cluster configuration high-availability

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group

Note - You must run this command in Gaia gClish.

Description

Shows cluster configuration - High Availability values.

Related Commands

- *"set cluster configuration high-availability" on page 925*

Syntax

```
show cluster configuration high-availability<ESC><ESC>
```

```
show cluster configuration high-availability
      bond <Name of Bond> min_slaves
      down_on_first_join
      factors member
      factors pnote pingable_hosts
      factors port bond
      factors port mgmt
      factors port other
      factors port standard
      factors sensor cmm
      factors sensor fans
      factors sensor power_supplies
      factors sensor ssm
      failover
      freeze_interval
      mgmt-monitoring
      mode
      port <Name of Port> priority
      vs
```

Parameters

Parameter	Description
`bond <Name of Bond> min_slaves`	Shows the minimum number of subordinate interfaces in the "UP" state in the specified bond interface. If the number of subordinate interfaces in the "UP" state is lower than the configured threshold, then the cluster state of this bond interface changes to "DOWN".
`down_on_ first_join`	Shows whether a Security Group Member must remain in the Administratively Down state when it joins the Security Group. ■ 0 - Does **not** enable the administratively DOWN state for the first join. ■ 1 - Enables the administratively DOWN state for the first join. See: ■ For ElasticXL Cluster and Maestro, see *"Setting the Administratively DOWN State on First Join" on page 571*. ■ For Scalable Chassis, see *"Setting the Administratively DOWN State on First Join in Dual Chassis" on page 387*.
`factors member`	Shows the Grade factor for the component "Security Group Member".
`factors pnote pingable_ hosts`	Shows the Grade factor for the component "Critical Device 'Pingable Hosts'".
`factors port bond`	Shows the Grade factor factor for the component "Bond Interfaces".
`factors port mgmt`	Shows the Grade factor for the component "Management Ports".
`factors port other`	Shows the High Grade factor for the component "Ports".
`factors port standard`	Shows the Standard Grade factor for the component "Ports".
`factors sensor cmm`	Shows the Grade factor for the component "CMMs" (only on Scalable Chassis).

Parameter	Description
`factors sensor fans`	Shows the Grade factor for the component "Fans" (only on Scalable Chassis).
`factors sensor power_ supplies`	Shows the Grade factor for the component "Power Supply Units" (only on Scalable Chassis).
`factors sensor ssm`	Shows the Grade factor for the component SSMs" (only on Scalable Chassis). This factor applies to all SSMs.
`failover`	Shows the minimum quality grade differential that causes a failover.
`freeze_ interval`	Shows the failover freeze interval. Valid freeze time values: ■ Value 0 - Disables this threshold. ■ Values 1-1000 - Specifies the freeze time in seconds. See the details in *"set cluster configuration high-availability" on page 925*.
`mgmt- monitoring`	Shows whether the monitoring of the Management Ports is enabled or disabled: ■ `on` - Enabled. ■ `off` - Disabled.
`mode`	Shows the Dual Site mode: ■ `0` - No primary Site ("Active Up" Mode) ■ `1` - "Primary Up" Mode ■ `2` - "Active Active" Mode ■ `3` - In the Traditional VSX mode, configures Virtual System Load Sharing (VSLS)
`port <Name of Port> priority`	Shows the Priority Level for the specified port: ■ `1` - Standard. ■ `2` - Other.

Parameter	Description

`vs`	Shows the priority for each Site for the current Traditional VSX Virtual System.
	You must run this command in the context of the applicable Virtual System.
	Example:
	`VS_ID = 0`
	`Weight = 10`
	`Number Of Standby = 1`
	`Priority List = 1 2`
	`Is Static Priority = 0`

show cluster configuration image

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows cluster settings - SMO Image Cloning.

Related Commands

- *"set cluster configuration image" on page 930*

Syntax

```
show cluster configuration image<ESC><ESC>
```

```
show cluster configuration image
      auto-clone state
      md5sum
```

Parameters

Parameter	Description
`auto-clone stat`	Shows whether the SMO Image Cloning is enabled or disabled in the Security Group.
`md5sum`	Shows the MD5 sum of the SMO Image.

show cluster configuration unique-ip

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows cluster settings - Unique IP Address per Site (UIPS).

For explanation, see:

- For ElasticXL Cluster / Maestro:

  "Configuring a Unique IP Address per Site (UIPS) in Maestro Dual Site" on page 208

- For Scalable Chassis:

  "Configuring a Unique IP Address per Site (UIPS) in Dual Chassis" on page 389

Related Commands

- *"set cluster configuration unique-ip" on page 931*
- *"delete cluster" on page 883*

Syntax

```
show cluster configuration unique-ip<ESC><ESC>
```

```
show cluster configuration unique-ip site-id <ID of Standby Site>
      interface <Name of Mgmt Interface>
```

Parameters

Parameter	Description
<ID of Standby Site>	Specifies the ID of the Standby Site / Standby Chassis: Valid values: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
<Name of Mgmt Interface>	Specifies the name of the Management Interface that is assigned to the Security Group. For example, `eth1-Mgmt1`.

show cluster info

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run this command in Gaia gClish.
- For the Expert mode, see *"cluster-cli" on page 863*.

Description

Shows cluster configuration.

Related Commands

- *"insights" on page 903*
- *"asg stat" on page 829*
- *"asg monitor (on Security Groups)" on page 792*
- *"cluster-cli" on page 863*
- *"set cluster" on page 920*

Syntax

```
show cluster info<ESC><ESC>
```

```
show cluster info
      connection [live] [src-ip <Source IP Address>] [dst-ip
<Destination IP Address>] [src-port <Source Port>] [dst-port
<Destination Port>] [protocol <Protocol Number>]
      cpu [live] [format json]
      interfaces [live] [format json]
      overview [live] [format json]
      pnotes [live] [format json]
      policy [live] [format json]
      provision [live] [format json]
      throughput [live] [format json]
```

Parameters

Parameter	Description
`connection [<Parameters>]`	Shows the current cluster connections.
`cpu <Parameters>`	Shows the CPU usage and the roles of the CPU cores. Available parameters: ■ `live` - Shows the output continuously. ■ `format json` - Shows the output in the JSON format.
`interfaces <Parameters>`	Shows information about the cluster interfaces: ■ Name ■ IP Address ■ Driver name ■ State ■ Throughput ■ Packet rate Available parameters: ■ `live` - Shows the output continuously. ■ `format json` - Shows the output in the JSON format.
`overview <Parameters>`	Shows the cluster overview information: ■ State of each Site ■ State of each Security Group Member ■ Throughput ■ Packet rate ■ Connection rate ■ Number of concurrent connections ■ Overall CPU usage ■ CoreXL split (Firewall instances / SND instances) ■ Overall CPU usage for CoreXL Firewall instances and SND instances ■ RAM usage ■ Which Critical Devices report their state as "`problem`" ■ State of Heart Beat Available parameters: ■ `live` - Shows the output continuously. ■ `format json` - Shows the output in the JSON format.

Parameter	Description
`pnotes` <*Parameters*>	Shows the Critical Devices that report their state as "`problem`". Available parameters: ■ `live` - Shows the output continuously. ■ `format json` - Shows the output in the JSON format.
`policy` <*Parameters*>	Shows information about the installed policy. Available parameters: ■ `live` - Shows the output continuously. ■ `format json` - Shows the output in the JSON format.
`provision` <*Parameters*>	Shows the provisioning state of new Security Group Members. You can see the progress if there are new Security Group Members that are joining the Security Group. Available parameters: ■ `live` - Shows the output continuously. ■ `format json` - Shows the output in the JSON format.
`throughput` <*Parameters*>	Shows the traffic throughput for the Management Interfaces and the Sync Interfaces. Available parameters: ■ `live` - Shows the output continuously. ■ `format json` - Shows the output in the JSON format.

Examples

Example 1 - 'show cluster info cpu'

```
[Global] SG-s01-01 > show cluster info cpu
Member 1_01

┌──────────┬──────────┬──────────┬──────────┬──────────┬──────────┬
──────────┬──────────┬──────────┐
│ Range/IDX │ 0        │ 1        │ 2        │ 3        │ 4        │
5        │ 6        │ 7        │

├──────────┼──────────┼──────────┼──────────┼──────────┼──────────┼
──────────┼──────────┼──────────┤
│ 0-7       │ [S] 2    │ [F] 34   │ [F] 40   │ [F] 41   │ [S] 1    │
[F] 35   │ [F] 35   │ [F] 36   │

└──────────┴──────────┴──────────┴──────────┴──────────┴──────────┴
──────────┴──────────┴──────────┘
Member 1_02

┌──────────┬──────────┬──────────┬──────────┬──────────┬──────────┬
──────────┬──────────┬──────────┐
│ Range/IDX │ 0        │ 1        │ 2        │ 3        │ 4        │
5        │ 6        │ 7        │

├──────────┼──────────┼──────────┼──────────┼──────────┼──────────┼
──────────┼──────────┼──────────┤
│ 0-7       │ [S] 0    │ [F] 11   │ [F] 15   │ [F] 16   │ [S] 0    │
[F] 15   │ [F] 16   │ [F] 11   │

└──────────┴──────────┴──────────┴──────────┴──────────┴──────────┴
──────────┴──────────┴──────────┘
Member 1_03

┌──────────┬──────────┬──────────┬──────────┬──────────┬──────────┬
──────────┬──────────┬──────────┐
│ Range/IDX │ 0        │ 1        │ 2        │ 3        │ 4        │
5        │ 6        │ 7        │

├──────────┼──────────┼──────────┼──────────┼──────────┼──────────┼
──────────┼──────────┼──────────┤
│ 0-7       │ [S] 1    │ [F] 17   │ [F] 16   │ [F] 13   │ [S] 1    │
[F] 20   │ [F] 21   │ [F] 20   │

└──────────┴──────────┴──────────┴──────────┴──────────┴──────────┴
──────────┴──────────┴──────────┘
CPU Type: (F) - FWK, (S) - SND, (O) - Other
[Global] SG-s01-01 >
```

Example 2 - 'show cluster info interfaces'

```
[Global] SG-s01-01 > show cluster info interfaces
┌──────────────────────────────────── Interfaces
──────────────────────────────────────┐
│
                    │
│  Name        │ IP Address     │ Driver           │ State │
Throughput │ Packet Rate  │
│
────────────┼────────────────┼────────────────┼────────┼──────────
───┼──────────────┤
│  ethsBP1-01 │                │ ixgbe            │ UP    │ 260.7K
    │ 148          │
│  ethsBP1-02 │                │ ixgbe            │ UP    │ 234.2K
    │ 120          │
│  BPEth0     │                │ bonding          │ UP    │ 260.7K
    │ 148          │
│  BPEth1     │                │ bonding          │ UP    │ 234.2K
    │ 120          │
│  eth1-06    │                │ Pseudo Ethernet │ UP    │ 232
    │ 0            │
│  eth1-07    │                │ Pseudo Ethernet │ UP    │ 0
    │ 0            │
│  eth1-11    │                │ Pseudo Ethernet │ UP    │ 88
    │ 0            │
│  eth2-06    │                │ Pseudo Ethernet │ UP    │ 112
    │ 0            │
│  eth2-07    │                │ Pseudo Ethernet │ UP    │ 0
    │ 0            │
│  eth2-11    │                │ Pseudo Ethernet │ UP    │ 1.6K
    │ 2            │
│  eth1-Mgmt1 │ 10.33.23.8/24 │ Pseudo Ethernet │ UP    │ 88.1K
    │ 55           │
│  bond4      │                │ bonding          │ UP    │ 352
    │ 0            │
│  bond2      │                │ bonding          │ UP    │ 1.7K
    │ 2            │
│  bond3      │                │ bonding          │ UP    │ 0
    │ 0            │
│
                    │

└──────────────────────────────────────────────────────────────────
──────────────────────┘
[Global] SG-s01-01 >
```

Example 3 - 'show cluster info overview'

```
[Global] SG-s01-01 > show cluster info overview
┌──────────────────────────────────────────────── Site 1 Standby
──────────────────────────────────────────────┐
│
                                              │
│  ID    │ Throughput │ Packet │ Conn. │ Conn. │ CPU    │ FW/SND │
FW/SND │ Mem.   │ State   │ Pnotes │ Heart   │
│        │            │ Rate   │ Rate  │       │ Usage │ Split   │
Usage   │ Usage │        │        │ Beat    │
│
───────┼────────────┼────────┼───────┼───────┼───────┼────────┼──
───────┼────────┼────────┼────────┼───────── │
│  1_01 │ 0          │ 0      │ 0     │ 51    │ 5     │ 12/8   │
8/0     │ 25     │ ACTIVE │ None   │ OK      │
│
                                              │

└──────────────────────────────────────────────────────────────────
──────────────────────────────────────────────┘
┌──────────────────────────────────────────────── Site 2 Active
──────────────────────────────────────────────┐
│
                                              │
│  ID    │ Throughput │ Packet │ Conn. │ Conn. │ CPU    │ FW/SND │
FW/SND │ Mem.   │ State   │ Pnotes │ Heart   │
│        │            │ Rate   │ Rate  │       │ Usage │ Split   │
Usage   │ Usage │        │        │ Beat    │
│
───────┼────────────┼────────┼───────┼───────┼───────┼────────┼──
───────┼────────┼────────┼────────┼───────── │
│  2_01 │ 0          │ 0      │ 0     │ 89    │ 4     │ 18/14  │
7/0     │ 27     │ ACTIVE │ None   │ OK      │
│
                                              │

└──────────────────────────────────────────────────────────────────
──────────────────────────────────────────────┘
[Global] SG-s01-01 >
```

Example 4 - 'show cluster info pnotes'

```
[Global] SG-s01-01 > show cluster info pnotes
┌─────────────┬──────┐
│ Member ID   │ Name │
├─────────────┼──────┤
│ 1_01        │ None │
│ 2_01        │ None │
└─────────────┴──────┘
[Global] SG-s01-01 >
```

Example 5 - 'show cluster info policy'

```
[Global] SG-s01-01 > show cluster info policy
┌─────────────┬──────────┬─────────────────────┬───────────┐
│ Member ID   │ Name     │ Time                │ Signature │
├─────────────┼──────────┼─────────────────────┼───────────┤
│ 1_01        │ Standard │ 2024-10-15 10:35:22 │ 21b8f0ef7 │
│ 2_01        │ Standard │ 2024-10-15 10:35:12 │ 21b8f0ef7 │
└─────────────┴──────────┴─────────────────────┴───────────┘
[Global] SG-s01-01 >
```

Example 6 - 'show cluster info throughput'

```
[Global] SG-s01-01 > show cluster info throughput
┌─────────────┬──────┬──────────┬──────┐
│ Member ID   │ Data │ Mgmt     │ Sync │
├─────────────┼──────┼──────────┼──────┤
│ 1_01        │ 0bps │ 944bps   │ 0bps │
│ 2_01        │ 0bps │ 299.2Kbps│ 0bps │
└─────────────┴──────┴──────────┴──────┘
[Global] SG-s01-01 >
```

show cluster site-id <ID> alert_threshold

This command is supported only on:

- Scalable Chassis

Note - You must run this command in Gaia gClish.

Description

Shows cluster settings - thresholds for hardware alerts.

Syntax

```
show cluster site-id <Site ID> alert_threshold<ESC><ESC>
```

```
set cluster site-id <Site ID> alert_threshold
      cpus_temperature_threshold_high
      cpus_temperature_threshold_low
      fans_threshold_high
      fans_threshold_low
      power_consumption_threshold_perc_high
      power_consumption_threshold_perc_low>
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
`cpus_temperature_threshold_high`	Shows the high threshold for CPU temperature (°C).
`cpus_temperature_threshold_low`	Shows the low threshold for CPU temperature (°C).
`fans_threshold_high`	Shows the high threshold for fans speed.
`fans_threshold_low`	Shows the low threshold for fans speed.
`power_consumption_threshold_perc_high`	Shows the high threshold for power consumption (%).
`power_consumption_threshold_perc_low`	Shows the low threshold for power consumption (%).

Related Commands

- *"set cluster site-id <Site ID> alert_threshold" on page 941*
- *"set cluster alert_threshold" on page 921*
- *"show cluster alert_threshold" on page 957*
- *"delete cluster" on page 883*

show cluster site-id <Site ID> general

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows cluster configuration - general user-defined settings.

Syntax

```
show cluster site-id <Site ID> general<ESC><ESC>
```

```
show cluster site-id <Site ID> general
      snmp_retries
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
`snmp_retries`	Shows the number of retries before timeout.

Related Commands

- *"set cluster site-id <Site ID> general" on page 943*
- *"delete cluster" on page 883*

show cluster site-id <Site ID> module

This command is supported only on:

- Scalable Chassis

Note - You must run this command in Gaia gClish.

Description

Shows cluster configuration - hardware components on Scalable Chassis..

Syntax

```
show cluster site-id <Site ID><ESC><ESC>
```

```
show cluster site-id <Site ID> module <Module>
            ip
            ports_amount
            secondary_ip
            snmp_auth
            status
            username
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: ■ `1` - Site #1 ■ `2` - Site #2 ■ `all` - All Sites
<Module>	Specifies the hardware module: ■ `CMM` - CMMs ■ `SSM1` - SSM #1 ■ `SSM2` - SSM #2 ■ `SSM3` - SSM #3 ■ `SSM4` - SSM #4 ■ `Mgmt` - Management Ports
`ip` *<IP Address>*	Shows the primary IP address. Applies only to the SSM modules.

Parameter	Description
`ports_amount <Number>`	Shows the number of ports. Applies only to the SSM and Management Ports modules.
`secondary_ip <IP Address>`	Shows the secondary IP address. Applies only to the CMM modules.
`snmp_auth <Algorithm>`	Shows the SNMP Authentication algorithm. Applies only to the SSM and Management Ports modules.
`status`	Shows the status. Applies only to the SSM and Management Ports modules.
`username`	Shows the internal username. Applies only to the SSM and Management Ports modules.

Examples

Example 1 - Primary IP address of SSM1

```
[Global] SG-s01-01 > show cluster site-id all module SSM1 ip
1_01:
Site 1 SSM1 IP 198.51.100.32
Site 2 SSM1 IP 198.51.100.32

1_02:
Site 1 SSM1 IP 198.51.100.32
Site 2 SSM1 IP 198.51.100.32

1_03:
Site 1 SSM1 IP 198.51.100.32
Site 2 SSM1 IP 198.51.100.32

1_04:
Site 1 SSM1 IP 198.51.100.32
Site 2 SSM1 IP 198.51.100.32
[Global] SG-s01-01 >
```

Related Commands

- *"set cluster site-id <Site ID> module" on page 944*
- *"set cluster site-id <Site ID> modules_amount" on page 946*
- *"asg hw_monitor" on page 1051*
- *"delete cluster" on page 883*

Example 2 - Number of Management Ports

```
[Global] SG-s01-01 > show cluster site-id all module Mgmt ports_
amount
1_01:
Site 1 Mgmt ports amount 2
Site 2 Mgmt ports amount 2

1_02:
Site 1 Mgmt ports amount 2
Site 2 Mgmt ports amount 2

1_03:
Site 1 Mgmt ports amount 2
Site 2 Mgmt ports amount 2

1_04:
Site 1 Mgmt ports amount 2
Site 2 Mgmt ports amount 2
[Global] SG-s01-01 >
```

Example 3 - Status of Management Ports

```
[Global] SG-s01-01 > show cluster site-id all module Mgmt status
1_01:
Site 1 Mgmt status active
Site 2 Mgmt status active

1_02:
Site 1 Mgmt status active
Site 2 Mgmt status active

1_03:
Site 1 Mgmt status active
Site 2 Mgmt status active

1_04:
Site 1 Mgmt status active
Site 2 Mgmt status active
[Global] SG-s01-01 >
```

show cluster site-id <Site ID> modules_amount

This command is supported only on:

- Scalable Chassis

Note - You must run this command in Gaia gClish.

Description

Shows cluster configuration - the required number of hardware components.

Syntax

```
show cluster site-id <Site ID> modules_amount<ESC><ESC>
```

```
show cluster site-id <Site ID> modules_amount
      cmm
      fans
      power_units
      ssm
```

Parameters

Parameter	Description
<Site ID>	Specifies the Site ID: - `1` - Site #1 - `2` - Site #2 - `all` - All Sites
`cmm`	Shows the required number of Chassis Management Modules (CMMs).
`fans`	Shows the required number of Fans.
`power_units`	Shows the required number of Power Supply Units (PSU).
`ssm`	Shows the required number of Security Switch Modules (SSMs).

Examples from Scalable Chassis 64000

Example 1 - CMMs

```
[Global] SG-s01-01 > show cluster site-id all modules_amount cmm
1_01:
Site 1 CMMs required amount 2
Site 2 CMMs required amount 2

1_02:
Site 1 CMMs required amount 2
Site 2 CMMs required amount 2

1_03:
Site 1 CMMs required amount 2
Site 2 CMMs required amount 2

1_04:
Site 1 CMMs required amount 2
Site 2 CMMs required amount 2
[Global] SG-s01-01 >
```

Example 2 - Fans

```
[Global] SG-s01-01 > show cluster site-id all modules_amount
fans
1_01:
Site 1 Fans required amount 6
Site 2 Fans required amount 6

1_02:
Site 1 Fans required amount 6
Site 2 Fans required amount 6

1_03:
Site 1 Fans required amount 6
Site 2 Fans required amount 6

1_04:
Site 1 Fans required amount 6
Site 2 Fans required amount 6
[Global] SG-s01-01 >
```

Example 3 - Power Supply Units

```
[Global] SG-s01-01 > show cluster site-id all modules_amount
power_units
1_01:
Site 1 Power units required amount 5
Site 2 Power units required amount 5

1_02:
Site 1 Power units required amount 5
Site 2 Power units required amount 5

1_03:
Site 1 Power units required amount 5
Site 2 Power units required amount 5

1_04:
Site 1 Power units required amount 5
Site 2 Power units required amount 5
[Global] SG-s01-01 >
```

Example 4 - SSMs

```
[Global] SG-s01-01 > show cluster site-id all modules_amount ssm
1_01:
Site 1 SSMs required amount 2
Site 2 SSMs required amount 2

1_02:
Site 1 SSMs required amount 2
Site 2 SSMs required amount 2

1_03:
Site 1 SSMs required amount 2
Site 2 SSMs required amount 2

1_04:
Site 1 SSMs required amount 2
Site 2 SSMs required amount 2
[Global] SG-s01-01 >
```

Related Commands

- *"set cluster site-id <Site ID> modules_amount" on page 946*
- *"show cluster site-id <ID> alert_threshold" on page 975*
- *"set cluster site-id <Site ID> alert_threshold" on page 941*
- *"asg hw_monitor" on page 1051*
- *"delete cluster" on page 883*

show cluster vsls

This command is supported only on these:

- Maestro Security Group in the Traditional VSX mode
- Scalable Chassis Security Group in the Traditional VSX mode

Note - You must run this command in Gaia gClish.

Description

Shows cluster configuration - in the Traditional VSX mode, shows the Virtual System Load Sharing (VSLS) settings.

Syntax

```
show cluster vsls<ESC><ESC>
```

```
show cluster vsls
      member_ratio
      system
            mgmt_monitoring
            primary_site
```

Parameters

Parameter	Description
`member_ratio`	Shows the VSLS cluster member ratio.
`system mgmt_ monitoring`	Shows which Virtual Systems monitor the Management Port link state: ■ `VS0_only` Only VS0 monitors the link state of the Management Port. Failover occurs only for VS0 and the SMO. ■ `all_VSs` All Virtual Systems decide their state based on link state of the Management Port. Failover occurs for all Virtual Systems.

Parameter	Description
`system primary_site`	Shows the VSLS Primary Site: ■ `0` - The Security Group decides automatically, based on the Virtual System ID. ■ `1` - Site 1 is the primary Site. ■ `2` - Site 2 is the primary Site.

Related Commands

- *"set cluster vsls" on page 948*
- *"set cluster configuration high-availability" on page 925*
- *"show cluster configuration high-availability" on page 960*

show distribution

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows the settings for the Distribution Mode.

See *"Working with the Distribution Mode" on page 554*.

Related Commands

- *"set distribution" on page 950*

Syntax

```
show distribution
      configuration
      interface <Name of Interface> configuration
      l4-mode
      matrix-max-size
      matrix-size [mode {general | user-network | per-port} ipv6
{on | off} spi {on | off} l4-mode {on | off} mtx-max-size {1k | 2k
| 4k | 8k | 16k}]
      spi mode
      status [verbose]
      verification [verbose]
```

Commands

Command	Description
`show distribution configuration`	Shows the Distribution Configuration.
`show distribution interface`	Shows the Interface Distribution Mode settings.
`show distribution l4-mode`	Shows the Layer 4 Distribution Mode settings.
`show distribution matrix-max-size`	Shows the maximum size of the Distribution Mode Matrix.
`show distribution matrix-size`	Shows the maximum current size of the Distribution Mode Matrix. You can specify different mode parameters.
`show distribution spi mode`	Shows the status of the SPI Distribution Mode.
`show distribution status [verbose]`	Shows the Distribution Mode status.
`show distribution verification [verbose]`	Shows the results of the Distribution Mode verification test.

show smo

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows settings related to the Single Management Object (SMO) on the Security Group.

Related Commands

- *"add smo" on page 824*
- *"set smo" on page 954*
- *"delete smo" on page 886*

Syntax

```
show smo
      audit-log expert-mode
      log <Log File> [from "<Timestamp>"] [to "<Timestamp>"] [tail
<N>] [filter "<String>"]
      security-group
            sgm-weight VALUE
            site-amount
      user-defined
            sync-file
```

Commands

Command	Description
`show smo audit-log expert-mode`	Shows the whether the audit logs for SMO operations in the Expert mode are enabled or disabled.
`show smo log <Log File> [<Filter Parameters>]`	Shows the content of log files aggregated from all Security Group Members. See *"asg log" on page 775*.
`show smo security-group`	On a Maestro Security Group with different Security Appliances, shows the configured weights for Security Group Members to balance the traffic proportionally. See *"Configuring Weights for Security Group Members in Maestro" on page 174*.
`show smo user-defined sync-file`	Shows the synchronization status of the user-defined files. See the explanation in *"set smo" on page 954*.

tcpdump

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run the "`g_tcpdump`" command in the Expert mode
- You must run the "`tcpdump`" command in Gaia gClish.

Description

This command performs the Multi-Blade Traffic Capture.

It captures and shows 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
`tcpdump -mcap`	Saves packets from specified Security Group Members to a capture file.
`tcpdump -view`	Shows packets from the specified capture file, including the Security Group Member ID.

Syntax in the Expert mode

```
g_tcpdump [-b <SGM IDs>] -mcap -w <Output File> [<tcpdump Options>]
```

```
g_tcpdump -view -r <Input File> [<tcpdump Options>]
```

Syntax in Gaia gClish

```
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
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

`-w <Output File>`	Saves the captured packets at the specified path in a file with the specified the name.
	This output file contains captured packets from all specified Security Group Members.
	In the same directory, the command saves additional output files for each Security Group Member.
	The names of these additional files are: `<SGM ID>_<Specified Name of Output File>`
	Example:
	■ The specified full path is:
	`/tmp/capture.cap`
	■ The additional capture files are:
	`/tmp/1_1_capture.cap`
	`/tmp/1_2_capture.cap`
	`/tmp/1_3_capture.cap`
	and so on

`-r <Input File>`	Reads the captured packets (in the `tcpdump` format) from the specified path from a file with the specified the name.
`<tcpdump Options>`	Standard `tcpdump` parameters. See the `tcpdump` manual page - https://linux.die.net/man/8/tcpdump.

Examples

Example 1 - Capture packets on all Security Group Members

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > 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] SG-s01-01>
```

Example 2 - Capture packets from specified Security Group Members and interfaces

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > tcpdump -b 1_1,1_3,2_1 -mcap -w /tmp/capture.cap -nnni eth1-Mgmt4
... ...
[Global] SG-s01-01 >
```

Example 3 - Show captured packets from a file

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01> 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] SG-s01-01>
```

Related Commands

- FW Monitor - see the *R82 CLI Reference Guide* > Chapter "Security Gateway Commands" > Section "fw" > Section "fw monitor".
- CPPCAP - see sk141412 - Check Point Traffic Capture Tool.

update_conf_file

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Notes:

- You must run the "`update_conf_file`" command in Gaia gClish.
- You must run the "`g_update_conf_file`" command the Expert mode.

Description

Adds, updates, and removes parameters in the specified configuration file.

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

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 `$FWDIR/boot/modules/fwkern.conf` and `$PPKDIR/conf/simkern.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 (*"asg_cp2blades" on page 730*).

Related Commands

- *"fw ctl get" on page 888*
- *"fw ctl set" on page 890*

Syntax

Syntax for Gaia gClish

```
update_conf_file <File Name> <Parameter Name>=<Parameter Value>
```

Syntax for the Expert mode

```
g_update_conf_file <File Name> <Parameter Name>=<Parameter Value>
```

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
<File Name>	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): ■ `$FWDIR/boot/modules/fwkern.conf` ■ `$PPKDIR/conf/simkern.conf`
<Parameter Name>	Name of the parameter to configure.
<Parameter Value>	New value for the parameter to configure.

Examples

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01>
[Global] SG-s01-01> update_conf_file /home/admin/MyConfFile.txt var1=hello
[Global] SG-s01-01>
[Global] SG-s01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=hello

[Global] SG-s01-01> update_conf_file /home/admin/MyConfFile.txt var2=24h
[Global] SG-s01-01>
[Global] SG-s01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=hello

[Global] SG-s01-01> update_conf_file /home/admin/MyConfFile.txt var1=goodbye
[Global] SG-s01-01>
[Global] SG-s01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=goodbye

[Global] SG-s01-01> update_conf_file /home/admin/MyConfFile.txt var2=
[Global] SG-s01-01>
[Global] SG-s01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=goodbye
[Global] SG-s01-01>
```

ver

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You must run this command in Gaia gClish.

Description

Shows the Security Group software version.

Related Commands

- *"asg_version" on page 1068* (only for Scalable Chassis)

Syntax

```
ver
```

Examples

```
[Global] SG-s01-01 > ver
1_01:
Product version Check Point Gaia R82
OS build xxx
OS kernel version 4.18.0-372.9.1cpx86_64
OS edition 64-bit

1_02:
Product version Check Point Gaia R82
OS build xxx
OS kernel version 4.18.0-372.9.1cpx86_64
OS edition 64-bit

[Global] SG-s01-01 >
```

CLI Commands for Maestro Orchestrator

add maestro

This command is supported only on:

- Maestro Orchestrator

Note - You must run this command in Gaia Clish.

Description

Adds items to Security Groups on the Maestro Orchestrator.

Related Commands

- *"show maestro" on page 1034*
- *"set maestro" on page 1027*
- *"delete maestro" on page 1012*

Syntax

```
add maestro [Esc] [Esc]
```

```
add maestro auto-scale security-group-id <ID>
      scale-down-policy when <Trigger> with <Metric> less-than
<Threshold> period <Duration>
      scale-up-policy when <Trigger> with <Metric> more-than
<Threshold> period <Duration>
```

```
add maestro lsp group <1-1024> [port <Port1>,<Port2>,...]
```

```
add maestro port <Name> vlan <ID>
```

```
add maestro security-group id <ID>
      interface <Name>
      site-id <ID> serial <Serial Number>
```

Commands

Command	Description
`add maestro auto-scale`	Configures the Auto-Scaling settings. See *"Maestro Auto-Scaling" on page 217*.
`add maestro lsp group <1-1024> [port <Port1>,<Port2>,...]`	Creates a Link State Propagation (LSP) Group and adds ports to this LSP Goup. See *"Configuring Link State Propagation (LSP) on a Maestro Orchestrator" on page 258*.
`add maestro port <Name> vlan <ID>`	Adds a VLAN on the port.
`add maestro security-group id <ID>`	Adds an unassigned item to a Security Group. ■ `interface <Name>` Add an unassigned interface to the Security Group. ■ `site-id <ID> serial <Serial Number>` Add an unassigned Security Appliance to the Security Group.

asg monitor (on Maestro Orchestrator)

This command is supported only on:

- Maestro Orchestrator

Note - You can run this command in Gaia Clish or in the Expert mode.

Description

Continuously shows the status of the Security Appliances and to which Security Groups they are assigned.

To stop the monitor session, press **CTRL+C**.

The command output shows:

- Security Group ID
- Maestro Site ID
- Security Group Member ID
- Security Appliance's Serial Number
- Security Appliance's State (Active, Unassigned, or "N/A")
- Security Appliance's Hardware Model
- Security Appliance's Software Version

Related Commands

- *"asg stat" on page 829*

Syntax

```
asg monitor -h
```

```
asg [-s <1-100>]] monitor ["Unassigned"]
```

Parameters

Parameter	Description
No Parameters	Shows the output.
`-h` `--help`	Shows the built-in help.
`"Unassigned"`	Shows the output only for the unassigned Security Appliances.
`-s <1-100>` `--sample_rate <1-100>`	Configures the data refresh interval (in seconds) for this session. Default is 1 second.

cplink

This command is supported only on:

- Maestro Orchestrator

Note - You must run this command in the Expert mode.

Description

Shows advanced information about the ports on the Maestro Orchestrator.

See sk180812.

Related Commands

- *"orch_stat" on page 1017*

Syntax

```
cplink -h
```

```
cplink [-j] [-r] <Port>
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-j` `--json`	Shows the output in the JSON format.

Parameter	Description
`-r` `--raw`	Shows the additional details. Output may not contain values for all these parameters. **Additional details** ■ `Group Opcode` ■ `Status Opcode` ■ `Attenuation` ■ `Bias Current` ■ `CDR RX` ■ `CDR TX` ■ `Compliance` ■ `FW Version` ■ `LOS Alarm` ■ `Power Class` ■ `Rx Power Current` ■ `Temperature` ■ `Tx Power Current` ■ `Voltage` ■ `Wavelength`
<Port>	Specifies the port to inspect. One of these: ■ A physical port: *<Port Number>* Example: `cplink 1` ■ A port label: *<Orchestrator ID>/<Port Label>* Example: `cplink 1/1` ■ A port label with subport: *<Orchestrator ID>/<Port Label>/<Port Split ID>* Example: `cplink 1/1/1` If the port is not split with a break-out cable, then enter the Port Number as it appears on the Orchestrator's front panel. If a break-out cable is connected to a port, then enter the applicable numbers: ■ For Split 1, enter *<Port Label>* ■ For Split 2, enter *<Port Label>*`/2` ■ For Split 3, enter *<Port Label>*`/3` ■ For Split 4, enter *<Port Label>*`/4`

Examples

Example 1 - Standard output

```
[Expert@MHO1_1:0]# orch_stat -p

Ports Status
+---------------+----------------+-----------+-----+-----------
+-------------+------------+-------------------+----------------
-+-------+-----------+-----------+
| Physical Port | Interface Name | Type      | SG  | QSFP Mode |
Admin State | Link State | Transceiver State | Operating Speed |
MTU   | RX Frames | TX Frames |
+---------------+----------------+-----------+-----+-----------
+-------------+------------+-------------------+----------------
-+-------+-----------+-----------+
| 1/1/1         | eth1-Mgmt1     | Mgmt      | 1   | 10G       |
UP          | UP         | PLUGGED           | 10GB_CR         |
10240 | 155831054 | 104498732 |
|               |                |           | 2   |           |
            |            |                   |                 |
      |           |           |
+---------------+----------------+-----------+-----+-----------
+-------------+------------+-------------------+----------------
-+-------+-----------+-----------+
...
[Expert@MHO1_1:0]#

[Expert@MHO1_1:0]# cplink 1/1/1

Troubleshooting Info
====================
Recommendation:                No issue was observed

Module Info
===========
Cable Technology:              Passive
Cable Type:                    Passive copper cable
Digital Diagnostic Monitoring: No
Identifier:                    SFP28/SFP+
OUI:                           Other
Rev:                           A0
Transfer Distance [m]:         1
Vendor Name:                   Gigalight
Vendor Part Number:            GPP-PC192-3001CP
Vendor Serial Number:          GE18190037

Operational Info
================
```

```
Auto Negotiation:                ON
FEC:                             No FEC
Loopback Mode:                   No Loopback
Physical state:                  LinkUp
Speed:                           10GbE
State:                           Active
Width:                           1x

Supported Info
==============
Enabled Link Speed:              10G
Supported Cable Speed:           10G, 1G

EYE Opening Info
================
Height Eye Opening [mV]:         246
Phase  Eye Opening [psec]:       0
Physical Grade:                  18149

Tool Information
================
Firmware Version:                13.2012.2140
MFT Version:                     mft 4.26.1-3
[Expert@MHO1_1:0]#
```

Example 2 - Raw output

```
[Expert@MHO1_1:0]# orch_stat -p

Ports Status
+---------------+----------------+-----------+-----+-----------
+-------------+-----------+------------------+----------------
-+-------+-----------+-----------+
| Physical Port | Interface Name | Type      | SG  | QSFP Mode |
Admin State | Link State | Transceiver State | Operating Speed |
MTU   | RX Frames | TX Frames |
+---------------+----------------+-----------+-----+-----------
+-------------+-----------+------------------+----------------
-+-------+-----------+-----------+
| 1/1/1         | eth1-Mgmt1     | Mgmt      | 1   | 10G       |
UP          | UP         | PLUGGED           | 10GB_CR         |
10240 | 155831054 | 104498732 |
|               |                |           | 2   |           |
            |            |                   |                 |
      |           |           |
+---------------+----------------+-----------+-----+-----------
+-------------+-----------+------------------+----------------
-+-------+-----------+-----------+
...
[Expert@MHO1_1:0]#

[Expert@MHO1_1:0]# cplink 1/1/1 -r

Troubleshooting Info
====================
Group Opcode:                   N/A
Recommendation:                 No issue was observed
Status Opcode:                  0

Module Info
===========
Attenuation (5g,7g,12g) [dB]:   N/A
Bias Current [mA]:              N/A
CDR RX:                         values: ['N/A']
CDR TX:                         values: ['N/A']
Cable Technology:               Passive
Cable Type:                     Passive copper cable
Compliance:                     N/A
Digital Diagnostic Monitoring:  No
FW Version:                     N/A
Identifier:                     SFP28/SFP+
```

```
LOS Alarm:                          N/A
OUI:                                Other
Power Class:                        N/A
Rev:                                A0
Rx Power Current [dBm]:             N/A
Temperature [C]:                    N/A
Transfer Distance [m]:              1
Tx Power Current [dBm]:             N/A
Vendor Name:                        Gigalight
Vendor Part Number:                 GPP-PC192-3001CP
Vendor Serial Number:               GE18190037
Voltage [mV]:                       N/A
Wavelength [nm]:                    N/A

Operational Info
================
Auto Negotiation:                   ON
FEC:                                No FEC
Loopback Mode:                      No Loopback
Physical state:                     LinkUp
Speed:                              10GbE
State:                              Active
Width:                              1x

Supported Info
==============
Enabled Link Speed:                 mask: 0x00007010, values:
['10G']
Supported Cable Speed:              mask: 0x00001001, values:
['10G', '1G']

EYE Opening Info
================
Height Eye Opening [mV]:            values: ['246']
Phase  Eye Opening [psec]:          values: ['0']
Physical Grade:                     values: ['18149']

Tool Information
================
Firmware Version:                   13.2012.2140
MFT Version:                        mft 4.26.1-3
[Expert@MHO1_1:0]#
```

delete maestro

This command is supported only on:

- Maestro Orchestrator

Note - You must run this command in Gaia Clish.

Description

Deletes items from Security Groups on the Maestro Orchestrator.

Related Commands

- *"show maestro" on page 1034*
- *"add maestro" on page 999*
- *"set maestro" on page 1027*

Syntax

```
delete maestro[Esc][Esc]
```

```
delete maestro authenticated mho <ID>
```

```
delete maestro auto-scale security-group-id <ID>
      scale-down-policy rule-id <ID>
      scale-up-policy rule-id <ID>
```

```
delete maestro configuration security-appliances inter-site vlan
translation security-group id <ID> custom vlan-id
```

```
delete maestro lsp group <1-1024> [port <Port1>,<Port2>,...]
```

```
delete maestro port <Name> vlan <VLAN ID>
```

```
delete maestro security-group
      id <ID>
            ftw-configuration
            interface <Name>
            management-connectivity
            site-id <ID> member <ID>
            site-id <ID> serial <Serial Number>
      new-config
```

Commands

Command	Description
`delete maestro authenticated mho <ID>`	Resets the authentication with the peer Orchestrators. See *"Authentication between Maestro Orchestrators" on page 85*.
`delete maestro auto-scale security-group-id <ID>`	Deletes the Auto-Scaling rules. See *"Maestro Auto-Scaling" on page 217*. ■ `scale-down-policy rule-id <ID>` ■ `scale-up-policy rule-id <ID>`
`delete maestro configuration security-appliances inter-site vlan translation security-group id <ID> custom vlan-id`	Deletes the user-defined VLAN ID for the Site-Sync VLAN translation for the Security Appliances. This restores the default VLAN ID.
`delete maestro lsp group <1-1024> [port <Port1>,<Port2>,...]`	Deletes the port from the LSP Group. Deletes the LSP Group. See *"Configuring Link State Propagation (LSP) on a Maestro Orchestrator" on page 258*.
`delete maestro port <Name> vlan <VLAN ID>`	Deletes a VLAN ID from the port.

Command	Description
`delete maestro security-group id <ID>`	Deletes the settings from the Security Group. ■ `ftw-configuration` Deletes the First Time Configuration Wizard settings. ■ `interface <Name>` Deletes the interface. ■ `management-connectivity` Deletes the Management Interface settings. ■ `site-id <ID> member <ID>` Deletes the Security Appliance, specified by its ID. ■ `site-id <ID> serial <Serial Number>` Deletes the Security Appliance, specified by its Serial Number.
`delete maestro security-group new-config`	Deletes the new configuration for Security Groups that was not applied yet.

orch_info

This command is supported only on:

- Maestro Orchestrator

Note - You must run this command in the Expert mode.

Description

Collects diagnostic information from the Maestro Orchestrator.

Syntax

```
orch_info -h
```

```
orch_info
      -h
      -f <Path to Output File>
      -c <Category>
```

Parameters

Parameter	Description
`-h` `--help`	Shows the built-in help.
`-f <Path to Output File>` `--filepath <Path to Output File>`	Specifies the path to the output TGZ file.
`-c <Category>` `--custom <Category>`	Specifies the category of additional information to collect. See the `/etc/orch_info_conf.yaml` file.

Examples

```
[Expert@MHO1_1:0]# orch_info
Collecting information, this may take a few minutes.
Compressing log files (Done)
Compressing conf files (Done)
Running diagnostics (Done)
Running more diagnostics (Done)
Compressing conf files (Done)
Compressing folders (Done)

Filepath: /home/admin/SG1_20_10_2024_21_41.tar.gz
[Expert@MHO1_1:0]#
```

orch_stat

This command is supported only on:

- Maestro Orchestrator

Note - You can run this command in Gaia Clish or in the Expert mode.

Description

Shows information about the Maestro Orchestrator.

Related Commands

- *"cplink" on page 1003*

Syntax

```
orch_stat -h
```

```
orch_stat -x
```

```
orch_stat
      -a
      -A
      -c
      -d
      -D {port | interface | sg | gw} <Object Name> [<Object Name
2> ...]
      -j
      -l
      -L
      -M {port | sg | gw}
      -p
      -q
      -t
      -v
      -V {vlan | port_id | interface | lag_id } <Object Name>
[<Object Name 2> ...]
      sample_rate <Number of Seconds> <Object Name> [<Object Name
2> ...]
```

Parameters

Parameter	Description
`-h` `--help`	Shows the built-in help.

`-x`
`--print_`
`examples`
	Shows the usage examples.

<Object Name>	Specifies the applicable object for specific commands (you can specify more than one object): ■ To specify a Port Name, use this format: *<Orchestrator ID>/<Port Label>/<Subport Label>* ■ To specify a Port ID, use this format: <0xHexDecPortID> ■ To specify a Security Group ID, use this format: *<Security Group ID>* ■ To specify a Security Group Member, use this format: *<Security Group ID>_<Site ID>_<Security Group Member ID>* ■ To specify an Interface Name, use one of these formats: • eth*<Number>*-*<Number>* • eth*<Number>*-Mgmt*<Number>* • ethsBP*<Number>*-*<Number>* • SYNC-INT • SYNC-EXT ■ To specify a VLAN ID, use this format: *<VLAN ID>* ■ To specify a LAG (Link Aggregation) ID, use this format: <0xHexDecLAGID>
`-a` `--all`	Shows all information from all categories.

`-A`
`--`
`authentication`
	Shows the authentication status for this Orchestrator.

`-c` `--console`	Shows the output in the format that is more suitable for a console connection.

Parameter	Description
`-d` `--deployment`	Shows the deployment and device data for this Orchestrator. Shows these columns in the output in the "`MHO Device Status`" section: ■ `Device Type` (the hardware model of the Orchestrator) ■ `Serial Number` (the serial number of the Orchestrator) ■ `MAC Address (UID)` (the MAC Address of the Orchestrator - the first "**Mgmt**" port) Shows these columns in the output in the "`MHO Deployment Information`" section: ■ `MHO ID` (Full ID of the Orchestrator - <Site ID>_<Orchestrator ID>) ■ `Site ID` (ID of the Maestro Site) ■ `Member ID` (ID of the Orchestrator on its Site) ■ `Number of MHOs on site` (number of Orchestrators on this Site) ■ `Number of Sites` (number of Maestro Sites)

`-D <`*`Parameters`*`>`
`--discard_counters`
<*Parameters*>
	Shows the discard counters for the specified objects.
	■ `-D port <`*`Port Name of Port ID`*`>`
	Specifies a port object.
	To see the Port Names and Port IDs, run "`orch_stat --ports`".
	■ `-D sg <`*`Security Group ID`*`>`
	Specifies a Security Group object.
	■ `-D gw <`*`Security Group ID`*`>/<`*`Site ID`*`>/<`*`Security Group Member ID`*`>`
	Specifies a Security Group Member object.

`-j` `--json`	Shows output in the JSON format.
`-l` `--lag`	Shows the LAG (Link Aggregation) information.

Parameter	Description
	Shows these columns in the output in the "`MHO Sync LAGs (Bonds) Status`" section: ■ `Lag Name` (only in verbose output) ■ `Lag ID` (only in verbose output) ■ `Sync Type` (Local Site or Remote Site) ■ `Status` (up or down) ■ `Physical Ports` (<Orchestrator ID>/<Port ID>/<Split ID>) ■ `Ports ID` (internal port ID) ■ `Logical Port` (<Port ID> or <Split ID>) ■ `Link State` (up or down) ■ `Membership State` (active or inactive) ■ `Host Name` (hostname of the remote Orchestrator) ■ `Remote Interface` (name of the peer interface)
	Shows these columns in the output in the "`Gateway LAGs (Bonds) Status`" section: ■ `SG` (ID of the Security Group) ■ `GW` (ID of the Security Group Member) ■ `Status` (up or down) ■ `LSP State` (forward or drop) ■ `Ports ID` (internal port ID) ■ `Logical Port` (<Port ID> or <Split ID>) ■ `Physical Ports` (<Orchestrator ID>/<Port ID>/<Split ID>) ■ `Link State` (up or down) ■ `Membership State` (active or inactive) ■ `Serial` (serial number of the Security Group Member) ■ `Remote Interface` (name of the peer interface) ■ `Host Name` (hostname of the remote Security Group Member) ■ `Internal IP`

Parameter	Description
`-L` `--LLDP`	Shows the LLDP information. The Security Appliances send LLDP packets to the Orchestrator. Based on these LLDP packets, the Orchestrator maintains the internal database of the Security Appliances and the Orchestrator ports, to which they are connected. Shows these columns in the output: ■ `Physical Port`(<Orchestrator ID>/<Port ID>/<Split ID>) ■ `Logical Port` (<Port ID> or <Split ID>) ■ `Hostname` (hostname of the Security Group Member) ■ `Type` ("`GW`" or "`---`") ■ `ID` (serial number of the Security Group Member, only in verbose output) ■ `HW Type` (hardware model of the Security Group Member) ■ `Version` (software version of the Security Group Member) ■ `State` (active or inactive) ■ `IP` (internal IP address of the Security Group Member) ■ `Remote Interface` (name of the peer interface, only in verbose output)
`-M <`*`Parameters`* `--traffic_monitor <`*`Parameters`*	Show live monitoring of throughput and packet rate. ■ `-D port <`*`Port Name of Port ID`*`>` Specifies a port object. To see the Port Names and Port IDs, run "`orch_stat --ports`". ■ `-D sg <`*`Security Group ID`*`>` Specifies a Security Group object. ■ `-D gw <`*`Security Group ID`*`>/<`*`Site ID`*`>/<`*`Security Group Member ID`*`>` Specifies a Security Group Member object.

Parameter	Description
`-p` `--ports`	Shows information about Orchestrator ports. Shows these columns in the output: ■ `Physical Port` (<Orchestrator ID>/<Port ID>/<Split ID>) ■ `Logical Port` (<Port ID> or <Split ID>, only in verbose output) ■ `Port ID` (internal port ID, only in verbose output) ■ `Interface Name` (interface name in Gaia OS) ■ `Type` (Management, Uplink, Downlink, Site Sync, SSM Sync) ■ `SG` (ID of the Security Group) ■ `QSFP Mode` (port speed) ■ `Admin State` (up or down) ■ `Link State` (up or down) ■ `Transceiver State` (plugged or unplugged) ■ `Auto Negotiation` (enabled or disabled, only in verbose output) ■ `Operating Speed` ■ `MTU` ■ `RX Frames` ■ `TX Frames`
`-q` `--quick`	Shows only information that is quick to retrieve.
`-t` `--topology`	Shows the topology information for Security Groups. Also see *"asg monitor (on Maestro Orchestrator)" on page 1001*.
`-v` `--verbose`	Shows verbose output.

Parameter	Description

`-V <Parameters`
`--vlan`
`<Parameters`
	Shows VLAN assignments.
	■ `-V vlan {all | <VLAN ID 1> <VLAN ID 2> ... <VLAN ID N>`
	Specifies a VLAN ID object.
	■ `-V port_id {all | <Port ID 1> <Port ID 2> ... <Port ID N>`
	Specifies a Port ID object.
	To see the Port IDs, run "`orch_stat --ports`".
	■ `-V interface <Name 1> <Name 2> ... <Name N>`
	Specifies an interface object.
	The name is one of these:
	• `eth<N>-<N>`
	• `eth<N>-Mgmt<N>`
	• `ethsBP<N>-<N>`
	• `SYNC-INT`
	• `SYNC-EXT`
	To see the interface names, run "`orch_stat --ports`".
	■ `-V lag_id {all | <LAG ID 1> <LAG ID 2> ... <LAG ID N>`
	Specifies a LAG (Link Aggregation) ID object.
	To see the LAG IDs, run "`orch_stat --lag`".

	Shows these columns in the output in the "`VLAN's ports`" section: ■ `VLAN ID` ■ `Port ID` (internal port ID) ■ `Interface Name` ■ `Type` (Management, Uplink, Downlink) ■ `Tagged Member` (true or false) Shows these columns in the output in the "`VLAN's LAGs`" section: ■ `VLAN ID` ■ `LAG ID` ■ `LAG Name` ■ `Tagged Member` (true or false)
`sample_rate` `<Parameters`	Specifies the interval (in seconds) between samples.

Usage Examples

```
[Expert@MyOrch_1:0]# orch_stat -x
Usage Examples:
        all: orch_stat -a [-v] [-j]
        authentication: orch_stat -A [-v] [-j]
        deployment: orch_stat -d [-j]
        LLDP: orch_stat -L [-v] [-j]
        ports: orch_stat -p [-v] [-j]
        topology: orch_stat -t [-j]
        discard_counters:
                option 1: orch_stat -D port 1/32/1 1/1/1 [-j]
                option 2: orch_stat -D port all [-j]
                option 3: orch_stat -D interface eth2-Mgmt1 SYNC-
EXT ethsBP1-02 eth2-29 [-j]
                option 4: orch_stat -D gw 1_2_1 3_2_1 [-j]
                option 5: orch_stat -D sg 1 2 3
                option 6: orch_stat -D sg all [-j]
        lag:
                option 1: orch_stat [-v] [-j]
                option 2: orch_stat -l [-v] [-j]
        traffic_monitor:
                option 1: orch_stat -M port 2/32/1
                option 2: orch_stat -M gw 1_2_1 3_2_1 [-v]
                option 3: orch_stat -M sg 1 2 3 sample_rate 5 [-v]
        vlan:
                option 1: orch_stat -V port_id 0x13d00 0x11f00 [-
v] [-j]
                option 2: orch_stat -V port_id all [-v] [-j]
                option 3: orch_stat -V vlan 1 2 100 [-v] [-j]
                option 4: orch_stat -V vlan all [-v] [-j]
                option 5: orch_stat -V interface  ethsBP1-02 eth2-
21 eth1-Mgmt1 SYNC-INT [-v] [-j]
                option 6: orch_stat -V lag_id  0x10000100
0x10000300 [-v] [-j]
                option 7: orch_stat -V lag_id  all [-v] [-j]
        print_examples: orch_stat -x
        console: orch_stat -c [-v]
[Expert@MyOrch_1:0]#
```

orchd

This command is supported only on:

- Maestro Orchestrator

Note - You must run this command in the Expert mode

Description

Controls the main daemon (`orchd`) on the Maestro Orchestrator.

Warning - No traffic flows through the Maestro Orchestrator until this daemon starts.

Related Commands

- *"orch_stat" on page 1017*

Syntax

```
orchd help
```

```
orchd
      activate
      restart
      start
      status
      stop
```

Parameters

Parameter	Description
`--help`	Shows the built-in help.
`activate`	Activate the Maestro Orchestrator. To enable the Uplink ports and the required daemons, you must manually activate your Orchestrator in these cases: ■ If you performed a clean install. ■ You restored the Orchestrator to its factory defaults. For more information, see sk171784.
`restart`	Restarts the daemon.
`start`	Starts the daemon.
`status`	Shows the status of the daemon (up or down).
`stop`	Stops the daemon.

set maestro

This command is supported only on:

- Maestro Orchestrator

Note - You must run this command in Gaia Clish.

Description

Configures settings on the Maestro Orchestrator.

Related Commands

- *"show maestro" on page 1034*
- *"add maestro" on page 999*
- *"delete maestro" on page 1012*

Syntax

```
set maestro[Esc][Esc]
```

```
set maestro auto-scale
      security-group-id <ID>
            scale-units-to-attach <Number>
            state {enable | disable}
      site-id <ID> scale-unit-serial <Serial Number> state {on |
off}
```

```
set maestro configuration
      hft state {enabled | disabled}
      orchestrator-amount <Number>
      orchestrator-member-id <ID>
      orchestrator-site-amount <Number>
      orchestrator-site-id <ID>
      orchestrators base-vlan <VLAN ID>
      security-appliances inter-site
            base-vlan <VLAN ID>
            vlan encapsulation {enabled | disabled}
            vlan translation security-group id <ID> custom vlan-id
<VLAN ID>
            vlan translation state {enabled | disabled}
      uplink-trunk-mode state {enabled | disabled}
      vxlan state {enabled | disabled}
```

```
set maestro export
      local orchestrator configuration archive-name <File Name>
path <Path>
      remote orchestrator id <ID> configuration archive-name <File
Name> path <Path>
```

```
set maestro gateway serial <VALUE> description <VALUE>
```

```
set maestro import configuration archive-name <File Name> path
<Path>
```

```
set maestro lsp
      apply
      group <1-1024> ports <Port1>,<Port2>,...
      revert
      state {on | off}
```

```
set maestro port <Name>
      admin-state {up | down}
      auto-negotiation {enabled | disabled}
      blink {0 | <1-60>}
      mtu <72-10240>
      qsfp-mode {1G | 10G | 25G | 40G | 100G}
      type {management | uplink | downlink | site_sync | ssm_sync}
[no-confirmation]
```

```
set maestro security-group
      apply-new-config [no-confirmation]
      id <ID>
            description "<Text>"
            ftw-configuration hostname <Hostname> sic <Activation
Key> is-vsx {no | yes} [admin-password <Password>]
            interface <Name> description "<Text>"
            management-connectivity ipv4-address <IPv4 Address>
mask-length <Mask Length> [default-gw <VALUE> create-mgmt-as-bond
{no | yes bond-mode {active-backup | xor | 8023AD}}]
            shared-uplinks state {enabled | disabled}
            site-id <ID>
                  description "<Text>"
                  member <ID> description "<Text>"
```

```
set maestro snmp traps port-state {on | off}
```

Commands

Command	Description
`set maestro auto-scale`	Configures the Auto-Scaling settings. See *"Maestro Auto-Scaling" on page 217*.

Command	Description
`set maestro configuration`	Configures the Orchestrator settings. ■ `hft state {enabled | disabled}` Configures the high frequency trading configuration. ■ `orchestrator-amount <Number>` Configures the number of Orchestrators in this Maestro deployment. ■ `orchestrator-member-id <ID>` Configures the Orchestrator Member ID on its Site. ■ `orchestrator-site-amount <VALUE>` Configures the number of Sites in this Maestro deployment. ■ `orchestrator-site-id <ID>` Configures the Site ID. ■ `orchestrators base-vlan <VLAN ID>` Configures the Orchestrator's base VLAN ID. ■ `security-appliances inter-site base-vlan <VLAN ID>` Configures the base VLAN ID for the Security Appliance communication between Sites. ■ `security-appliances inter-site vlan encapsulation {enabled | disabled}` Configures the state of the Site-Sync VLAN encapsulation for the Security Appliances. ■ `security-appliances inter-site vlan translation security-group id <ID> custom vlan-id <VLAN ID>` Configures the user-defined VLAN ID for the Site-Sync VLAN translation for the Security Appliances. ■ `security-appliances inter-site vlan translation state {enabled | disabled}` Configures the state of the Site-Sync VLAN translation for the Security Appliances. ■ `uplink-trunk-mode state {enabled | disabled}` Configures the state of the Uplink Trunk Mode. ■ `vxlan state {enabled | disabled}` Configures the state of VXLAN.

Command	Description
`set maestro export`	Exports the Orchestrator configuration to an archive file. ■ `local orchestrator configuration archive-name <File Name> path <Path>` Exports the Orchestrator configuration on the current Orchestrator on this Site, to which you are connected. ■ `remote orchestrator id <ID> configuration archive-name <File Name> path <Path>` Exports the Orchestrator configuration on the remote Orchestrator on another Site.
`set maestro import configuration`	Imports the Orchestrator configuration from the specified archive file on the current Orchestrator.
`set maestro lsp`	Configures the Link State Propagation (LSP) settings. See *"Configuring Link State Propagation (LSP) on a Maestro Orchestrator" on page 258*.

Command	Description
`set maestro port <Name>`	Configures the port settings. ■ `admin-state {up | down}` Configures the port administrative state. ■ `auto-negotiation {enabled | disabled}` Configures the port auto-negotiation state. ■ `blink {0 | <1-60>}` Forces the port's LED to blink for the specified number of seconds (0 to disable). ■ `mtu <72-10240>` Configures the port MTU. ■ `qsfp-mode {1G | 10G | 25G | 40G | 100G}` Configures the port QSFP mode (port speed). **Warning** - There are ports on Orchestrators that support only specific speeds. See the *Maestro Getting Started Guide* > Chapter "Hardware Components". ■ `type {management | uplink | downlink | site_sync | ssm_sync} [no-confirmation]` Configures the port type. The parameter "`no-confirmation`" is optional. If specified, the command does not ask you for confirmation and audit information. **Warning** - There are ports on Orchestrators that support only specific types. See the *Maestro Getting Started Guide* > Chapter "Hardware Components".
`set maestro security-group apply-new-config [no-confirmation]`	Applies the new configuration for Security Groups that was not applied yet. The parameter "`no-confirmation`" is optional. If specified, the command does not ask you for confirmation and audit information.

Command	Description
`set maestro security-group <ID>`	Configures the Security Group settings. ■ `description "<Text>"` Configures the description for this Security Group. ■ `ftw-configuration hostname <Hostname> sic <Activation Key> is-vsx {no | yes} [admin-password <Password>]` Configures the First Time Configuration Wizard settings. On Orchestrator R82 and higher, if you configure "`is-vsx yes`", then: • A Security Group R82 and higher runs in the VSNext mode. • A Security Group R80.20SP - R81.20 runs in the Traditional VSX mode. ■ `interface <Name> description "<Text>"` Configures the description for the interface. ■ `management-connectivity ipv4-address <IPv4 Address> mask-length <Mask Length> [default-gw <VALUE> create-mgmt-as-bond {no | yes bond-mode {active-backup | xor | 8023AD}}]` Configures the Management Interface in the Security Group. ■ `shared-uplinks state {enabled | disabled}` Configures the Shared Uplinks state. See *"Shared Uplink Ports on a Maestro Security Group" on page 200*. ■ `site-id <ID> description "<Text>"` Configures the description for the Site. ■ `site-id <ID> member <VALUE> description "<Text>"` Configures the description for the Orchestrator on the Site.
`set maestro snmp traps port-state {on | off}`	Configures the state of the SNMP traps for Orchestrator ports.

show maestro

This command is supported only on:

- Maestro Orchestrator

Note - You must run this command in Gaia Clish.

Description

Shows settings on the Maestro Orchestrator.

Related Commands

- *"add maestro" on page 999*
- *"set maestro" on page 1027*
- *"delete maestro" on page 1012*

Syntax

```
show maestro[Esc][Esc]
```

```
show maestro auto-scale
      interactive-rules
      interactive-status
      scale-units
      security-group-id <ID>
            scale-down-rules
            scale-up-rules
            state
```

```
show maestro configuration
      hft state
      orchestrator-amount
      orchestrator-member-id
      orchestrator-site-amount
      orchestrator-site-id
      orchestrators base-vlan
      security-appliances inter-site
            base-vlan
            vlan encapsulation
            vlan translation
      uplink-trunk-mode state
      vxlan state
```

```
show maestro gateway serial <Serial Number> description
```

```
show maestro lsp
      configuration {all | group <1-1024>}
      history <1-1000>
      status
```

```
show maestro port <Name>
      admin-state
      admin-state
      auto-negotiation
      mtu
      optic-info
      optic-info-details
      qsfp-mode
      type
      vlans
```

```
show maestro security-group id <ID>
      description
      interface <Name> description
      shared-uplinks state
      site-id <ID>
            description
            member <ID> description
```

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

```
show maestro snmp traps port-state
```

Commands

Command	Description
`show maestro auto-scale`	Shows the Auto-Scaling settings. See *"Maestro Auto-Scaling" on page 217*. ■ `interactive-rules` Shows the status of the Auto-Scaling rules in realtime. ■ `interactive-status` Shows the status of the Auto-Scaling in Security Groups in realtime. ■ `scale-units` Shows the configured scale units. ■ `scale-down-rules` Shows the Scale-Down policy. ■ `scale-up-rules` Shows the Scale-Up policy. ■ `state` Shows the Auto-Scaling state.

Command	Description
`show maestro configuration`	Shows the Orchestrator settings. ■ `hft state` Show high frequency trading configuration. ■ `orchestrator-amount` Shows the number of configured Orchestrators in this Maestro deployment. ■ `orchestrator-member-id` Shows the configured Orchestrator Member ID on its Site. ■ `orchestrator-site-amount` Shows the number of configured Sites in this Maestro deployment. ■ `orchestrator-site-id` Shows the configured Orchestrator Site ID. ■ `orchestrators base-vlan` Shows the Orchestrator's base VLAN ID. ■ `security-appliances inter-site base-vlan` Shows the base VLAN ID for the Security Appliance communication between Sites. ■ `security-appliances inter-site vlan encapsulation` Shows the state of the Site-Sync VLAN encapsulation for the Security Appliances. ■ `security-appliances inter-site vlan translation` Shows the Site-Sync VLAN translation configuration for the Security Appliances. ■ `uplink-trunk-mode state` Shows the state of the Uplink Trunk Mode. ■ `vxlan state` Shows the state of VXLAN.
`show maestro gateway serial <Serial Number> description`	Shows the configured description for the selected Security Appliance. Press the TAB key to see the detected Serial Numbers.
`show maestro lsp`	Shows the Link State Propagation (LSP) settings. See *"Configuring Link State Propagation (LSP) on a Maestro Orchestrator" on page 258*.

Command	Description
`show maestro port <Name>`	Shows the settings for the specified port. Press the TAB key to select the required port. ■ `admin-state` Shows the port administrative state. ■ `auto-negotiation` Shows the port auto-negotiation state. ■ `mtu` Shows the port MTU. ■ `optic-info` Shows information about the QSFP transceiver inserted in the port. ■ `optic-info-details` Shows detailed information about the QSFP transceiver inserted in the port. ■ `qsfp-mode` Shows the port QSFP mode (port speed). ■ `type` Shows the port type - Management, Uplink, Downlink, Internal Sync (`site_sync`), External Sync (`ssm_sync`). ■ `vlans` Deprecated command Related commands: ■ *"orch_stat" on page 1017* ■ *"cplink" on page 1003*

Command	Description
`show maestro security-group id <ID>`	Shows ■ `description` Shows the configured description for this Security Group. ■ `interface <Name of Interface> description` Shows the configured description for the interface. ■ `shared-uplinks state` Shows the Shared Uplinks configuration. See *"Shared Uplink Ports on a Maestro Security Group" on page 200*. ■ `site-id <ID> description` Shows the configured description for the Site. ■ `site-id <ID> member <ID> description` Shows the configured description for the Orchestrator on the Site.
`show maestro security-group verify-new-config`	Verifies the new configuration for Security Groups that was not applied yet.
`show maestro snmp traps port-state`	Shows the state of the SNMP traps for Orchestrator ports.

CLI Commands for Scalable Chassis

asg_chassis_ctrl

This command is supported only o:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Use the Scalable Chassis Control utility to monitor and configure (Security Switch Modules) SSMs and (Chassis Management Modules) CMMs with different commands and parameters.

The Scalable Chassis Control utility is based on SNMP communication between the Scalable Chassis.

Related Commands

- *"asg_hard_reboot" on page 1045*
- *"asg_hard_shutdown" on page 1047*
- *"asg_hard_start" on page 1049*
- *"asg_jumbo_conf" on page 1057*

Syntax

```
asg_chassis_ctrl <Option> <Parameters>
```

Notes:

- To see the full syntax for an option, enter the command and option without parameters.
- To make sure the Scalable Chassis Control commands work correctly in a Dual Chassis configuration, run this command on each Scalable Chassis.

Parameters

Options and Parameters	Description
`help [-v]`	Shows help messages in Verbose Mode.

Options and Parameters	Description
`active_sgms`	Shows all installed SGMs.
`active_ssm`	Shows active SSMs. An SSM that is not installed or is in the DOWN state, does not appear as Active.
`get_fans_status`	Shows the health status of the Scalable Chassis fans.
`get_lb_dist {<SSM ID> | all}`	Shows the current distribution matrix from the specified SSM or all SSMs. The matrix is a table containing SGM IDs and used to determine to which other SGMs a packet should be forwarded.
`get_ssm_firmware {<SSM ID> | all}`	Shows the firmware version of the specified SSM or all SSMs.
`get_ssm_type {<SSM ID> | all}`	Shows the model of the specified SSM or all SSMs.
`get_psu_status`	Shows the current status of the AC PSUs.
`get_pems_status`	Shows the current status of the DC PEMs.
`get_cmm_status`	Shows the current status of the CMMs.
`get_cpus_temp <SGM ID>`	Shows temperatures of the specified SGM CPUs.
`get_dist_md5sum`	Shows the MD5 of the distribution matrix for the given SSM. Comparing this checksum against the checksum on other SSMs and verifies that they are synchronized.
`get_ports_stat <SSM ID>`	Prints the port status for the specified SSM.
`get_dist_mode <SSM ID>`	Shows the port Distribution Mode for the specified SSM.
`get_dist_mask <SSM ID>`	Shows a summary of the distribution masks in the different modes.
`get_matrix_size <SSM ID>`	Shows the size, in bytes, of the SSM distribution matrix.

Options and Parameters	Description
`get_sel_info <CMM ID>`	Shows data from the specified CMM event. This information is useful for troubleshooting and system forensics.
`restart_ssm <SSM IDgt;`	Restarts the specified SSM.
`restart_cmm <CMM ID>`	Restarts the specified CMM.
`start_ssm <SSM ID>`	Starts the specified SSM.
`shutdown_ssm <smm_id>`	Shuts down the specified SSM.
`mib2_stats <SSM ID> <Port ID> [<Error Type>]`	Shows MIB2 statistics for the specified SSM and port.
`get_bmac <SSM ID>`	Shows SGM MAC addresses from the SSM.
`get_power_type`	Shows the Chassis input power type (AC or DC).
`get_ac_power_type`	Shows the AC power type.
`jumbo_frames {enable | disable | show} <SSM ID>`	Enables, disables, or shows Jumbo Frames on SSM440. See *"Working with Jumbo Frames on Scalable Chassis" on page 361*.
`set_port_mtu <SSM ID> <Port ID> <MTU Size>`	Sets the port MTU size for the specified SSM and port. ■ *<SSM ID>* - SSM identifier (from `1` to `4`, or `all`) ■ *<Port ID>* - Port number ■ *<MTU Size>* - This MTU size can be one of these values: • An integer value up to 12,288 • `max` - Maximum supported MTU size • `default` - System default MTU size (typically, 1544)
`get_port_mtu <SSM ID> <Port ID>`	Shows the MTU for the specified SSM and port.
`get_port_media_details <SSM ID>`	Shows port information.
`get_pem_cb_status`	Shows DC PEM status.
`enable_port`	Enables the port.

Options and Parameters	Description
`disable_port`	Disables the port.

Examples

```
[Expert@SG-s01-01:0]# asg_chassis_ctrl get_cmm_status
Getting CMM(s) status
CMM #1 -> Health: 1, Active: 1
CMM #2 -> Health: 1, Active: 0
Active CMM firmware version: 2.83
[Expert@SG-s01-01:0]#
```

asg_hard_reboot

This command is supported only on:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

This command performs a hardware reboot of Security Gateway Modules (SGMs) on Scalable Chassis.

The CMM monitors and controls the Scalable Chassis components, activates, and shuts down SGMs and SSMs. Users can activate and shut down SGMs in serious situations. For example, when the Sync Interface cannot access the SGM. In that case, the `reboot` command does not work.

Notes:

- At least one SGM must be in the state "UP" to run this command.
- To learn how to restart an SSM from the CMM, see *"asg_chassis_ctrl" on page 1041*.

Related Commands

- *"asg_hard_shutdown" on page 1047*
- *"asg_hard_start" on page 1049*
- *"asg_reboot" on page 811*

Syntax

```
asg_hard_reboot -h
asg_hard_reboot [-a] -b <SGM IDs>
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-a`	Includes the Security Group Members that are in the "DOWN" state.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

asg_hard_shutdown

This command is supported only on:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

This command performs a hardware shutdown of Security Gateway Modules (SGMs) on Scalable Chassis.

The CMM monitors and controls the Scalable Chassis components, activates, and shuts down SGMs and SSMs. Users can activate and shut down SGMs in serious situations. For example, when the Sync Interface cannot access the SGM. In that case, the `reboot` command does not work.

Notes:

- At least one SGM must be in the state "UP" to run this command.
- To learn how to restart an SSM from the CMM, see *"asg_chassis_ctrl" on page 1041*.

Related Commands

- *"asg_hard_reboot" on page 1045*
- *"asg_hard_start" on page 1049*

Syntax

```
asg_hard_shutdown -h
asg_hard_shutdown [-a] -b <SGM IDs>
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-a`	Includes the Security Group Members that are in the "DOWN" state.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

asg_hard_start

This command is supported only on:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

This command performs a hardware start of Security Gateway Modules (SGMs) on Scalable Chassis.

The CMM monitors and controls the Scalable Chassis components, activates, and shuts down SGMs and SSMs. Users can activate and shut down SGMs in serious situations. For example, when the Sync Interface cannot access the SGM. In that case, the `reboot` command does not work.

Notes:

- At least one SGM must be in the state "UP" to run this command.
- To learn how to restart an SSM from the CMM, see *"asg_chassis_ctrl" on page 1041*.

Related Commands

- *"asg_hard_shutdown" on page 1047*
- *"asg_hard_reboot" on page 1045*

Syntax

```
asg_hard_start -h
asg_hard_start [-b <SGM IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Runs the command for all Security Group Members on the current Scalable Chassis.

Parameter	Description
`-b <SGM IDs>`	Specifies the Security Group Members, for which to run this command. Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)

asg hw_monitor

This command is supported only on:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows the hardware information and thresholds for the monitored components:

- For Chassis Management Modules (CMMs) - Installed, Active, or Standby
- For Security Switch Modules (SSMs) - Throughput rates
- For Security Gateway Modules (SGMs) - CPU temperature for each socket
- Power Supply Unit - Installed or not installed, and the PSU fan speed
- Speed of fans in Scalable Chassis
- Power consumption for each Scalable Chassis

Related Commands

- *"set cluster site-id <Site ID> alert_threshold" on page 941*
- *"show cluster site-id <ID> alert_threshold" on page 975*
- *"set cluster site-id <Site ID> modules_amount" on page 946*
- *"show cluster site-id <Site ID> modules_amount" on page 982*

Syntax

```
asg hw_monitor [-v] [-f <Filter>]
```

Parameters

Parameter	Description
`-v`	Shows detailed component status report (verbose)
`-f`	Show status of one or more specified (filtered) components
`<Filter>`	One or more of these component types, in a comma separated list: ■ `CMM` ■ `CPUtemp` ■ `Fan` ■ `PowerConsumption` ■ `PowerUnit` ■ `SSM`

Output Description

Column	Description
Location	Front panel location.
Value **Threshold** **Units**	Most components have a defined threshold value. The threshold gives an indication of the health and functionality of the component. When the value of the resource is greater than the threshold, the Scalable Chassis generates a system alert (see *"asg alert" on page 699*).
State	Valid values: ■ **0** = Component is not installed ■ **1** = Component is installed

Examples

Example output on a 64000 chassis

```
[Expert@SG-s01-01:0]# gclish
[Global] SG-s01-01 > asg hw_monitor -v
-------------------------------------------------------------------------------
| Hardware Monitor                                                            |
-------------------------------------------------------------------------------
| Sensor           | Location       | Value | Threshold | Units       | State |
-------------------------------------------------------------------------------
| Chassis 1                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 0     | 0         | <S,D>/<A>   | 1     |
| CMM              | bay 2          | 1     | 0         | <S,D>/<A>   | 1     |
| CPUtemp          | blade 1, CPU0  | 48    | 95        | Celsius     | 1     |
| CPUtemp          | blade 1, CPU1  | 47    | 95        | Celsius     | 1     |
| CPUtemp          | blade 2, CPU0  | 44    | 95        | Celsius     | 1     |
| CPUtemp          | blade 2, CPU1  | 48    | 95        | Celsius     | 1     |
| CPUtemp          | blade 3, CPU0  | 46    | 95        | Celsius     | 1     |
| CPUtemp          | blade 3, CPU1  | 48    | 95        | Celsius     | 1     |
| CPUtemp          | blade 4, CPU0  | 49    | 95        | Celsius     | 1     |
| CPUtemp          | blade 4, CPU1  | 51    | 95        | Celsius     | 1     |
| CPUtemp          | blade 5, CPU0  | 44    | 95        | Celsius     | 1     |
| CPUtemp          | blade 5, CPU1  | 47    | 95        | Celsius     | 1     |
| Fan              | bay 1, fan 1   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 1, fan 2   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 1, fan 3   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 2, fan 1   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 2, fan 2   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 2, fan 3   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 3, fan 1   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 3, fan 2   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 3, fan 3   | 4     | 11        | Speed Level | 1     |
| PowerConsumption | N/A            | 2461  | 11250     | Watts       | 1     |
| PowerUnit(AC)    | bay 1          | 0     | 0         | NA          | 1     |
| PowerUnit(AC)    | bay 2          | 0     | 0         | NA          | 1     |
| PowerUnit(AC)    | bay 3          | 0     | 0         | NA          | 0     |
| PowerUnit(AC)    | bay 4          | 0     | 0         | NA          | 1     |
| PowerUnit(AC)    | bay 5          | 0     | 0         | NA          | 1     |
| PowerUnit(AC)    | bay 6          | 0     | 0         | NA          | 1     |
| PowerUnitFan     | bay 1, fan 1   | 0     | 0         | NA          | 1     |
| PowerUnitFan     | bay 2, fan 1   | 0     | 0         | NA          | 1     |
| PowerUnitFan     | bay 3, fan 1   | 0     | 0         | NA          | 0     |
| PowerUnitFan     | bay 4, fan 1   | 0     | 0         | NA          | 1     |
| PowerUnitFan     | bay 5, fan 1   | 0     | 0         | NA          | 1     |
| PowerUnitFan     | bay 6, fan 1   | 0     | 0         | NA          | 1     |
| SSM              | bay 1          | 0     | 0         | Mbps        | 1     |
| SSM              | bay 2          | 0     | 0         | Mbps        | 1     |
-------------------------------------------------------------------------------
| Chassis 2                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 0     | 0         | <S,D>/<A>   | 1     |
| CMM              | bay 2          | 1     | 0         | <S,D>/<A>   | 1     |
| CPUtemp          | blade 1, CPU0  | 45    | 95        | Celsius     | 1     |
| CPUtemp          | blade 1, CPU1  | 46    | 95        | Celsius     | 1     |
| CPUtemp          | blade 2, CPU0  | 42    | 95        | Celsius     | 1     |
| CPUtemp          | blade 2, CPU1  | 47    | 95        | Celsius     | 1     |
| CPUtemp          | blade 3, CPU0  | 43    | 95        | Celsius     | 1     |
| CPUtemp          | blade 3, CPU1  | 43    | 95        | Celsius     | 1     |
| CPUtemp          | blade 4, CPU0  | 42    | 95        | Celsius     | 1     |
| CPUtemp          | blade 4, CPU1  | 42    | 95        | Celsius     | 1     |
| CPUtemp          | blade 5, CPU0  | 42    | 95        | Celsius     | 1     |
| CPUtemp          | blade 5, CPU1  | 45    | 95        | Celsius     | 1     |
| Fan              | bay 1, fan 1   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 1, fan 2   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 1, fan 3   | 4     | 11        | Speed Level | 1     |
| Fan              | bay 2, fan 1   | 4     | 11        | Speed Level | 1     |
```

```
| Fan              | bay 2, fan 2   | 4      | 11         | Speed Level | 1      |
| Fan              | bay 2, fan 3   | 4      | 11         | Speed Level | 1      |
| Fan              | bay 3, fan 1   | 4      | 11         | Speed Level | 1      |
| Fan              | bay 3, fan 2   | 4      | 11         | Speed Level | 1      |
| Fan              | bay 3, fan 3   | 4      | 11         | Speed Level | 1      |
| PowerConsumption | N/A            | 2130   | 9000       | Watts       | 1      |
| PowerUnit(AC)    | bay 1          | 0      | 0          | NA          | 1      |
| PowerUnit(AC)    | bay 2          | 0      | 0          | NA          | 1      |
| PowerUnit(AC)    | bay 3          | 0      | 0          | NA          | 0      |
| PowerUnit(AC)    | bay 4          | 0      | 0          | NA          | 1      |
| PowerUnit(AC)    | bay 5          | 0      | 0          | NA          | 1      |
| PowerUnit(AC)    | bay 6          | 0      | 0          | NA          | 0      |
| PowerUnitFan     | bay 1, fan 1   | 0      | 0          | NA          | 1      |
| PowerUnitFan     | bay 2, fan 1   | 0      | 0          | NA          | 1      |
| PowerUnitFan     | bay 3, fan 1   | 0      | 0          | NA          | 0      |
| PowerUnitFan     | bay 4, fan 1   | 0      | 0          | NA          | 1      |
| PowerUnitFan     | bay 5, fan 1   | 0      | 0          | NA          | 1      |
| PowerUnitFan     | bay 6, fan 1   | 0      | 0          | NA          | 0      |
| SSM              | bay 1          | 0      | 0          | Mbps        | 1      |
| SSM              | bay 2          | 0      | 0          | Mbps        | 1      |
-------------------------------------------------------------------------------
[Global] SG-s01-01 >
```

asg_jumbo_conf

This command is supported only on:

- Scalable Chassis

Note - You must run this command in the Expert mode.

Description

- Shows whether support for Jumbo Frames is enabled on Security Gateway Modules (SGMs).
- Shows whether support for Jumbo Frames is enabled on Security Switch Modules (SSMs).
- Shows the Jumbo Frames configuration on Security Switch Modules (SSMs).
- Enables and disables support for Jumbo Frames on Security Gateway Modules (SGMs).

See *"Working with Jumbo Frames on Scalable Chassis" on page 361*.

Related Commands

- *"asg_chassis_ctrl" on page 1041*

Syntax

```
asg_jumbo_conf
      -h
      enable
      disable
      show [-v]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`enable`	Enables support for Jumbo Frames on SGMs and SSMs.
`disable`	Disables support for Jumbo Frames on SGMs and SSMs. This is the default state.

Parameter	Description
`show [-v]`	Shows whether support for Jumbo Frames is enabled on SGMs and SSMs. The parameter "`-v`" also shows the current MTU.

Examples

```
[Expert@SG-s01-01:0]# asg_jumbo_conf show -v

Jumbo frames are disabled on SGMs (SSM1 max MTU: 1500 SSM2 max
MTU: 1500 )

Retrieving SSMs Jumbo frames configuration

Chassis1
▒▒▒▒▒▒▒▒▒
SSMs:
Jumbo frames are disabled on SSM1
Jumbo frames are disabled on SSM2

Interfaces MTU configuration:
The MTU of all the interfaces is 1500 or less.

Chassis2
▒▒▒▒▒▒▒▒▒
SSMs:
Jumbo frames are disabled on SSM1
Jumbo frames are disabled on SSM2

Interfaces MTU configuration:
The MTU of all the interfaces is 1500 or less.

[Expert@SG-s01-01:0]#

[Expert@SG-s01-01:0]# asg_jumbo_conf enable

Enabling Jumbo frames on SGMs
Enabling Jumbo Frames on SSMs
Chassis1
▒▒▒▒▒▒▒▒▒
Jumbo frames are enabled on SSM1
Jumbo frames are enabled on SSM2

Chassis2
▒▒▒▒▒▒▒▒▒
Jumbo frames are enabled on SSM1
Jumbo frames are enabled on SSM2


Jumbo frames enabled.
Don't forget to set the MTU of relevant interfaces in gclish.
[Expert@SG-s01-01:0]#
```

```
[Expert@SG-s01-01:0]# asg_jumbo_conf show -v

Jumbo frames are enabled on SGMs (SSM1 max MTU: 9416 SSM2 max MTU:
9416 )

Retrieving SSMs Jumbo frames configuration

Chassis1
▒▒▒▒▒▒▒▒▒▒
SSMs:
Jumbo frames are enabled on SSM1
Jumbo frames are enabled on SSM2

Interfaces MTU configuration:
interface:BPEth1:mtu 9416
interface:BPEth0:mtu 9416

The MTU of all the interfaces which are not in the list is 1500 or
less.

Chassis2
▒▒▒▒▒▒▒▒▒▒
SSMs:
Jumbo frames are enabled on SSM1
Jumbo frames are enabled on SSM2

Interfaces MTU configuration:
interface:BPEth1:mtu 9416
interface:BPEth0:mtu 9416

The MTU of all the interfaces which are not in the list is 1500 or
less.

[Expert@SG-s01-01:0]#
```

asg_serial_info

This command is supported only on these:

- ElasticXL Cluster
- Maestro Security Group
- Scalable Chassis Security Group

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

- On ElasticXL Cluster / Maestro:

  Shows the serial numbers of the Security Appliances.

- On Scalable Chassis

  Shows the serial numbers for the (Chassis Management Modules) CMMs, Security Switch Modules (SSMs), and Scalable Chassis.

  Note - To show the serial numbers for CMMs, SSMs and Scalable Chassis, one of the SGMs on each Scalable Chassis must be in the state "`UP`".
  For example, if no SGMs in the state "`UP`" are found on Chassis 2, the serial numbers for components in the Chassis are neither shown nor saved.

Related Commands

- *"asg_sgm_serial" on page 1064*

Syntax

```
asg_serial_info [-a]
```

Parameters

Parameter	Description
`-a`	Applies command to all Security Group Members in the Security Group.

Examples

Example 1 - Maestro

```
[Expert@SG-s01-01:0]# asg_serial_info
Collecting SGMs information...
+-------------------------+
|     Serial numbers      |
+------------+------------+
| Chassis ID |     1      |
| SGM1       | 1111111111 |
| SGM2       | 2222222222 |
| SGM3       | 3333333333 |
+------------+------------+
[Expert@SG-s01-01:0]#
```

Example 2 - Scalable Chassis

```
[Expert@SG-s01-01:0]# asg_serial_info
chassis 1 CMM1 serial: 1163978/005
chassis 1 CMM2 serial: 1157482/001
chassis 1 SSM1 serial: 0011140011
chassis 1 SSM2 serial: 0011140012
chassis 1 serial: 1159584/016
chassis 2 CMM1 serial: 1163090/041
chassis 2 CMM2 serial: 1155519/014
chassis 2 SSM1 serial: 0311310621
chassis 2 SSM2 serial: 0311310626
chassis 2 serial: 0831232/001
[Expert@SG-s01-01:0]#
```

asg_sgm_serial

This command is supported only on:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Shows and saves the serial numbers for the Security Gateway Modules (SGMs).

Notes:

- By default, the command runs only on SGMs in the state "`UP`".
- To show the serial numbers for CMMs, SSMs and Chassis, one of the SGMs on each Chassis must be in the state "`UP`".
  For example, if no SGMs in the state "`UP`" are found on Chassis 2, the serial numbers for components in the Chassis are not shown or saved.

Related Commands

- *"asg_serial_info" on page 1062*

Syntax

```
asg_sgm_serial [-a]
```

Parameters

Parameter	Description
`-a`	Applies command to all SGMs in the Security Group.

Examples

```
[Expert@SG-s01-01:0]# asg_sgm_serial
1_01:
 Board Serial          : AKO0769153
1_02:
 Board Serial          : AKO0585533
2_01:
 Board Serial          : AKO0462069
2_02:
 Board Serial          : AKO0447878
[Expert@SG-s01-01:0]#
```

asg_traffic_stats

This command is supported only on:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

Show traffic statistics for ports on Security Switch Modules (SSMs) during a specified time period:

- Throughput (Bits per second)
- Packet rate (packets per second)
- Packet rate statistics are divided to four categories:
- Unicast
- Multicast
- Broadcast
- Total packets per second

Syntax

```
asg_traffic_stats {<SSM ID> | <Name of SSM Interface>} [<Period>]
```

Parameters

Parameter	Description
<SSM ID>	Specifies the SSM ID - 1,2, 3, or 4.
<Name of Interface>	Specifies the name of the SSM interface.
<Period>	Specifies the time period, during which to collect the statistics. Default: 5 seconds.

Examples

```
[Expert@SG-s01-01:0]# asg_traffic_stats 1 2
Processing traffic statistics for 2 seconds...

Summary on SSM1
---------------
  Incoming traffic:
  -----------------
  Throughput: 48.0 Kbps
  Packet rate: [Total: 49 pps], [Unicast: 0 pps], [Multicast: 18
pps], [Broadcas
                                          t: 31 pps]

  Outgoing traffic:
  -----------------
  Throughput: 959.7 Kbps
  Packet rate: [Total: 1.3 Kpps], [Unicast: 0 pps], [Multicast: 0
pps], [Broadca
                                        st: 1.3 Kpps]

[Expert@SG-s01-01:0]#
```

asg_version

This command is supported only on:

- Scalable Chassis

Note - You can run this command in Gaia gClish or in the Expert mode.

Description

- Shows this information:
  - Check Point software version on the Security Gateway Modules (SGMs).
  - Firmware versions on the Security Gateway Modules (SGMs), Security Switch Modules (SSMs), and Chassis Management Modules (CMMs).
- Makes sure that system hardware components run approved software and firmware versions.

Related Commands

- *"ver" on page 998*

Syntax

```
asg_version -h
```

```
asg_version [verify] [-v] [-i] [-b <SGM IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`verify`	Makes sure that system hardware components run approved software and firmware versions.
`-i`	Shows Active and Standby SGMs.

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ One Site (`chassis1`, or `chassis2`) ■ The Active Site (`chassis_active`)
`-v`	Shows verbose version information.

Examples

Example 1 - Default output

```
[Expert@SG-s01-01:0]# asg_version

SGMs
======
OS version
----------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
OS build 776, OS kernel version 4.18.0-372.9.1cpx86_64, OS edition 64-bit

Hardware
--------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
BIOS: 2.28 BL: 1.00 IPMC: 1.02 FPGA: 2.34 NVRAM: 6.00

[Expert@SG-s01-01:0]#
```

Example 2 - Verbose output

```
[Expert@SG-s01-01:0]# asg_version -v
+-------------------------------------------------------------------------------+
| Hardware Versions                                                             |
+-------------------------------------------------------------------------------+
| Component       | Type            | Configuration      | Firmware           |
+-------------------------------------------------------------------------------+
| Chassis 1                                                                     |
+-------------------------------------------------------------------------------+
| SSM1            | SSM440          | N/A                | 5.5.R5.7.CP        |
| SSM2            | SSM440          | N/A                | 5.5.R5.7.CP        |
| CMM             | N/A             | N/A                | 3.70-rev6          |
+-------------------------------------------------------------------------------+

SGMs
======
Type
----------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
SGM400

OS version
----------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
OS build XXX, OS kernel version 4.18.0-372.9.1cpx86_64, OS edition 64-bit

FireWall-1 version
------------------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
This is Check Point's software version R82 - Build XXX
kernel: R82 - Build XXX

Performance Pack version
------------------------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
This is Check Point Performance Pack version: R82 - Build XXX
Kernel version: R82 - Build XXX

Installed Bundles
-----------------
-*- 1 blade: 1_01 -*-
BUNDLE_CORE_FILE_UPLOADER_AUTOUPDATE ...<truncated>
-*- 3 blades: 1_02 1_03 1_04 -*-
BUNDLE_CORE_FILE_UPLOADER_AUTOUPDATE ...<truncated>

Hardware
--------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
BIOS: 2.28 BL: 1.00 IPMC: 1.02 FPGA: 2.34 NVRAM: 6.00

SSD
---
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
Firmware Version: N2010112

Number of cores
---------------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
56

Number of CoreXL instances
--------------------------
-*- 4 blades: 1_01 1_02 1_03 1_04 -*-
52

CPUs frequency
--------------
```

```
-*- 3 blades: 1_01 1_03 1_04 -*-
2.4GHz
-*- 1 blade: 1_02 -*-
1.69GHz

[Expert@SG-s01-01:0]#
```

ccutil

This command is supported only on:

- Scalable Chassis

Note - You must run this command in the Expert mode.

Description

Shows and control hardware components in Scalable Chassis.

This is an advanced command for troubleshooting.

Warning - Do **not** change the settings with this command, unless Check Point Support explicitly told you to do so.

Syntax

```
ccutil -h
ccutil help -v
ccutil <Parameter>
```

Commands

Command	Description
`ccutil -h`	Shows the shortened built-in help with the description of each sub-command.
`ccutil help -v`	Shows the extended built-in help with the description of each sub-command.
`ccutil <Parameter>`	Runs the command for the specified parameter.

Parameters

Parameter	Category	Description
`ccutil -h`	N / A	Shows the shortened built-in help with the description of each sub-command.

Parameter	Category	Description
active_sgms	SGMs	Shows the active SGMs
active_ssm	SSMs	Shows the active SSMs
apply_dist_conf	Distribution	Applies the distribution configuration in the SSM
clear_mac_ learning	SSMs	Clears the MAC learning table on SSM (default: all)
disable_port	Ports	Disables the specified port
enable_port	Ports	Enables the specified port
get_ac_power_ type	PSU	Shows the AC power type
get_backplane_ admin_speed	SSMs	Shows the backplane ports admin speed
get_bmac	SSMs	Shows the MAC Addresses of SGMs from the SSM
get_cmm_status	CMMs	Shows the current status of the CMM(s)
get_cpus_temp	Other	Shows the temperatures of the CPUs of the specified SGMs
get_dist_mask	Distribution	Shows the a summery of the distribution masks in the different modes
get_dist_md5sum	Distribution	Shows the MD5 sum of the distribution matrix in the specified SSM
get_dist_mode	Distribution	Shows the SSM distribution mode
get_efm_oam_mode	SSMs	Shows the EFM-OAM protocol mode
get_fans_status	Fans	Shows the current status of the chassis fans
get_ipv6_mode	SSMs	Shows the IPv6 mode
get_l4_dist_mask	Distribution	Shows the L4 distribution masks
get_l4_dist_mode	Distribution	Shows the SSM L4 distribution mode
get_lb_dist	Distribution	Shows the current distribution Matrix from the specified SSM

Parameter	Category	Description
`get_lb_interfaces`	Distribution	Shows the VLAN LB interfaces
`get_lose_less_mode`	Other	Shows the loseless mode ratio
`get_matrix_size`	Distribution	Shows the distribution matrix size
`get_parity_error_counter`	SSMs	Shows the parity error counter of the SSM
`get_pem_cb_status`	PSU	Shows the circuit breaker status
`get_pems_status`	PSU	Shows the current status of the chassis PEM units
`get_port_admin_speed`	Ports	Shows the port administrative speed
`get_port_dist_mode`	Distribution	Shows the port distribution mode
`get_port_fec_state`	Ports	Shows the port FEC (Forward Error Correction) state
`get_port_media_details`	Ports	Shows the port transceiver
`get_port_mtu`	Ports	Shows the port MTU
`get_ports_stat`	Ports	Shows the ports status of the specified SSM
`get_power_type`	PSU	Shows the chassis power type (AC/DC)
`get_psu_status`	PSU	Shows the current status of the chassis power supply units
`get_qsfp_ports_mode`	Ports	Shows the QSFP mode
`get_sel_info [<File>]`	CMMs	Shows the SEL information from the CMM
`get_spi_mode`	Distribution	Shows the SPI based distribution mode
`get_ssm_firmware`	SSMs	Shows the firmware version of the specified SSM

Parameter	Category	Description
get_ssm_throughput	SSMs	Shows the overall throughput of the specified SSM
get_ssm_time	SSMs	Shows the time on specified SSM
get_ssm_type	SSMs	Shows the type the specified SSM
jumbo_frames	SSMs	Configures the Jumbo Frames on SSM
mib2_stats	Other	Shows the MIB2 statistics of the specified SSM
reload_ssm_default	SSMs	Reloads SSM manufacturing defaults
restart_cmm	CMMs	Restarts the specified CMM
restart_sgm	SGMs	Restarts the specified SGM
restart_ssm	SSMs	Restarts the specified SSM
set_backplane_speed	SSMs	Configures the backplane ports speed
set_bmac	SSMs	Configures the MAC Addresses of SGMs on the SSM
set_dist_mask	Distribution	Configures the distribution masks in the different modes
set_dist_mode	Distribution	Configures the SSM distribution mode
set_efm_oam_mode	SSMs	Configures the EFM-OAM protocol mode
set_ipv6_mode	SSMs	Configures the IPv6 mode
set_l4_dist_mask	Distribution	Configures the L4 distribution masks in the different modes
set_l4_dist_mode	Distribution	Configures the SSM L4 distribution mode
set_lb_dist	Distribution	Configures the distribution matrix with specified SGM IDs on specified SSM
set_lose_less_mode	Other	Configures the loseless mode ratio (1/64,1/32,1/16,1/8,1/4,1/2,1,2,4,8)

Parameter	Category	Description
`set_port_dist_mode`	Distribution	Configures the ports distribution mode
`set_port_fec_state`	Ports	Configures the port FEC (Forward error correction) state
`set_port_mtu`	Ports	Configures the port MTU
`set_port_speed`	Ports	Configures the port speed
`set_qsfp_ports_mode`	Ports	Configures the QSFP mode and restart SSM
`set_spi_mode`	Distribution	Configures the SPI based distribution mode
`shutdown_sgm`	SGMs	Shuts down the specified SGM
`shutdown_ssm`	SSMs	Shuts down the specified SSM
`ssm_exec`	SSMs	Runs the command on the SSM
`start_sgm`	SGMs	Starts the specified SGM
`start_ssm`	SSMs	Starts the specified SSM
`sync_ssm_time`	SSMs	Configures the current SGM time as specified SSM time

Glossary

A

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

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

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

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

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

B

Breakout Cable
An optical fiber cable that contains several jacketed simplex optical fibers that are packaged together inside an outer jacket. Synonyms: Fanout cable, Fan-Out cable, Splitter cable.

Bridge Mode
Check Point Firewall or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Chassis Management Module
On Scalable Chassis - a hardware component that controls and monitors 60000 / 40000 Appliance (Chassis) operation such as, fan speed, Chassis and module temperature, and component hot-swapping. Acronym: CMM.

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

Cluster
Two or more Check Point Firewalls that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Check Point Firewall that is part of a cluster.

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

Content Awareness
Software Blade on a Check Point Firewall that provides data visibility and enforcement. Acronym: CTNT.

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

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

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

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

D

DAC Cable
Direct Attach Copper cable. A form of the high-speed shielded twinax copper cable with pluggable transceivers on both ends. Used to connect to network devices (switches, routers, or servers).

DAIP Firewall
Check Point Firewall with a Dynamically Assigned IP (DAIP) is a server, on which the IP address of the external interface is assigned dynamically (by a DHCP server, by an ISP).

Data Loss Prevention
Software Blade on a Check Point Firewall that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

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

Distributed Deployment
Configuration in which the Check Point Firewall and the Security Management Server products are installed on different servers.

Downlink Ports
Interfaces on the Maestro Orchestrator used to connect to Check Point Security Appliances. You use DAC cables, Fiber cables (with transceivers), or Breakout cables to connect between the Downlink ports and Security Appliances. The Check Point Management traffic (policy, logs, synchronization, and so on) co-exists with the data (user) traffic on the Downlink ports. Bandwidth is guaranteed for the Check Point Management traffic (portion of the downlink bandwidth). These ports form the system backplane (management, data plane, synchronization).

Dynamic Object
Special object type, whose IP address is not known in advance. The Check Point Firewall resolves the IP address of this object in real time.

E

Endpoint Policy Management
Software Blade on a Management Server to manage an on-premises Endpoint Security environment.

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

G

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

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

Gaia gClish
The name of the global command line shell in Check Point Gaia operating system for Security Appliances connected to Check Point Maestro Orchestrators and for Security Gateway Modules on Scalable Chassis. Commands you run in this shell apply to all Security Gateway Module / Security Appliances in the Security Group.

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

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

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

HyperSync
Check Point patented technology that makes sure that active connections are only synchronized to backup Security Appliances in the Security Group. HyperSync makes sure each connection flow has a backup within the Security Group.

I

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

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

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

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

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

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

J

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

K

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

L

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

Logging & Status
Software Blade on a Management Server to view Security Logs from the managed Check Point Firewalls.

M

Maestro Orchestrator
A scalable Network Security System that connects multiple Check Point Security Appliances into a unified system. Synonyms: Orchestrator, Maestro Hyperscale Orchestrator. Acronym: MHO.

Management Interface
(1) Interface on a Gaia Check Point Firewall or Cluster Member, through which Management Server connects to the Check Point Firewall or Cluster Member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

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

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

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

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

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

N

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

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

O

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

Orchestrator
See "Maestro Orchestrator".

P

Power Entry Module
Hardware component that supplies DC power with EMC filtering and over-current protection on Scalable Chassis. Acronym: PEM.

Power Supply Unit
Hardware component that supplies AC power with filtering and over-current protection. Acronym: PSU.

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

Q

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

R

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

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

S

Scalable Chassis
The container that contains the all the components of a 60000 / 40000 Appliance. Synonym: Chassis.

SecureXL
Performance-enhancing technology on a Check Point Firewall that accelerates IPv4 and IPv6 traffic that passes through the Check Point Firewall.

Security Gateway Module
On Scalable Chassis - a hardware component on a 60000 / 40000 Appliance (Chassis) that operates as a physical Check Point Firewall. A Chassis contains many Security Gateway Modules that work together as a single, high performance Check Point Firewall or VSX Gateway. In Maestro - a role of a Security Appliance. Part of the Security Group that contains the assigned Security Appliances. A Security Appliance in a Security Group has one IPv4 address and represents all assigned Security Appliances as one entity. Acronym: SGM.

Security Group
A logical group of Security Appliances (in Maestro) / Security Gateway Modules (on Scalable Chassis) that provides Active/Active cluster functionality. A Security Group can contain one or more Security Appliances / Security Gateway Modules. Security Groups work separately and independently from each other. To the production networks, a Security Group appears a single Check Point Firewall. In Maestro, each Security Group contains: (A) Applicable Uplink ports, to which your production networks are connected; (B) Security Appliances (the Maestro Orchestrator determines the applicable Downlink ports automatically); (C) Applicable management port, to which the Check Point Management Server is connected.

Security Group Member
Member of a Security Group in ElasticXL Cluster, Maestro, and Scalable Chassis. Acronym: SGM.

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

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

Security Switch Module
On Scalable Chassis - a hardware component on a 60000 / 40000 Appliance (Chassis) that manages the flow of network traffic to and from the Security Gateway Module in the Chassis. In Maestro - a role of the Maestro Orchestrator that manages the flow of network traffic to and from the Security Groups. Acronym: SSM.

SGM
In Maestro - a role of a Security Appliance. Part of the Security Group that contains the assigned Security Appliances. A Security Appliance in a Security Group has one IPv4 address and represents all assigned Security Appliances as one entity. For Scalable Chassis - see "Security Gateway Module".

Shared Management
Feature that makes it possible to assign the same Management Port (interface ethX-MgmtY) on a Maestro Orchestrator to different Security Groups. The assigned Management Port has a different IP address and a different MAC address in each Security Group, to which this port is assigned.

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

Single Management Object
Single Check Point Firewall object in SmartConsole that represents a Security Group configured on a Maestro Orchestrator / Scalable Chassis. Acronym: SMO.

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

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

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

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

SMO Master
The Security Appliance (in Maestro) / Security Gateway Module (on Scalable Chassis) in a Security Group that handles management tasks for all Security Appliances / Security Gateway Modules in the Security Group. By default, this role is assigned to the Security Appliance / Security Gateway Module with the lowest Member ID in the Security Group. See "SMO".

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

SSM
In Maestro - a role of the Maestro Orchestrator that manages the flow of network traffic to and from the Security Groups. For Scalable Chassis - see "Security Switch Module".

Standalone
Configuration in which the Check Point Firewall and the Security Management Server products are installed and configured on the same server.

T

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

Threat Extraction
Software Blade on a Check Point Firewall that removes malicious content from files. Acronym: TEX.

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

U

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

Uplink Ports
Interfaces on the Maestro Orchestrator used to connect to external and internal networks. Gaia operating system shows these interfaces in Gaia Portal and in Gaia Clish. SmartConsole shows these interfaces in the corresponding SMO Check Point Firewall object.

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

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

V

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

Z

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