



15 July 2021

## INSTALLATION AND UPGRADE GUIDE

**R80.40**

# Check Point Copyright Notice

© 2020 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 R80.40



For more about this release, see the R80.40 [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
15 July 2021	<p>Updated:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing Software Packages on Gaia" on page 160</a></li> <li>■ <a href="#">"Upgrade Methods" on page 175</a></li> <li>■ <a href="#">"Management Server Migration Tool and Upgrade Tools" on page 182</a></li> <li>■ Added clarification notes in several procedures</li> </ul>
16 April 2021	<p>Updated:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing Full High Availability Cluster" on page 145</a></li> <li>■ The note "In a Management High Availability environment, the SmartEvent Software Blade is supported only on the <b>Active</b> Management Server (for more information, see <a href="#">sk25164</a>)."</li> </ul>
26 February 2021	<p>Added:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Multi-Version Cluster Upgrade Procedure - VSX Mode" on page 596</a></li> </ul> <p>Updated:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Backing Up and Restoring" on page 27</a> - added link to <a href="#">sk127653</a></li> <li>■ <a href="#">"Installing Software Packages on Gaia" on page 160</a></li> <li>■ <a href="#">"Prerequisites for Upgrading and Migrating of Management Servers and Log Servers" on page 164</a></li> <li>■ <a href="#">"Upgrading one Multi-Domain Server from R80.20 and higher" on page 305</a> - all procedures</li> <li>■ <a href="#">"Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with CPUSE" on page 359</a></li> <li>■ <a href="#">"Installing a VSX Gateway" on page 99</a> - updated notes</li> <li>■ <a href="#">"Installing a VSX Cluster" on page 123</a> - updated notes</li> <li>■ <a href="#">"Supported Versions in Multi-Version Cluster" on page 577</a></li> <li>■ <a href="#">"Multi-Version Cluster Upgrade Procedure - Gateway Mode" on page 581</a></li> </ul>
24 August 2020	<p>Added:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server" on page 681</a> (replaced the procedure "Changing the Leading Interface on Multi-Domain Server or Multi-Domain Log Server")</li> <li>■ <a href="#">"Changing the IP Address of a Domain Management Server or Domain Log Server" on page 687</a></li> <li>■ The note in upgrade procedures - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.</li> </ul>

Date	Description
	<p>Updated:</p> <ul style="list-style-type: none"> <li>■ "<a href="#">Installing a VSX Gateway</a>" on page 99</li> <li>■ "<a href="#">Installing a VSX Cluster</a>" on page 123</li> <li>■ "<a href="#">Prerequisites for Upgrading and Migrating of Management Servers and Log Servers</a>" on page 164</li> <li>■ "<a href="#">Upgrading Security Management Servers in Management High Availability from R80.10 and lower</a>" on page 207</li> <li>■ "<a href="#">Upgrading Security Management Servers in Management High Availability from R80.20 and higher</a>" on page 268</li> <li>■ "<a href="#">Upgrading a Dedicated Log Server from R80.10 and lower</a>" on page 212</li> <li>■ "<a href="#">Upgrading a Dedicated SmartEvent Server from R80.10 and lower</a>" on page 228</li> <li>■ "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher</a>" on page 244</li> <li>■ "<a href="#">Upgrading a Multi-Domain Log Server from R80.10 and lower</a>" on page 409</li> <li>■ "<a href="#">Upgrading a Multi-Domain Log Server from R80.20 and higher</a>" on page 430</li> <li>■ "<a href="#">Upgrading Multi-Domain Servers in High Availability from R80.10 and lower</a>" on page 323</li> <li>■ "<a href="#">Upgrading Multi-Domain Servers in High Availability from R80.20 and higher</a>" on page 358</li> <li>■ "<a href="#">Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower</a>" on page 482</li> <li>■ "<a href="#">Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher</a>" on page 499</li> <li>■ "<a href="#">Migrating Database from an R80.40 Security Management Server to an R80.40 Domain Management Server</a>" on page 643</li> <li>■ "<a href="#">Migrating Database from an R80.40 Domain Management Server to an R80.40 Security Management Server</a>" on page 647</li> <li>■ "<a href="#">Migrating Database from an R7x Domain Management Server to an R80.40 Domain Management Server</a>" on page 663</li> <li>■ "<a href="#">Migrating Database from an R7x Security Management Server to an R80.40 Domain Management Server</a>" on page 657</li> <li>■ "<a href="#">Migrating Database from an R7x Standalone to an R80.40 Domain Management Server</a>" on page 670</li> <li>■ "<a href="#">Upgrading one R7x Multi-Domain Server with Gradual Migration of Domain Management Servers</a>" on page 293</li> <li>■ "<a href="#">Upgrading a Security Gateway or VSX Gateway</a>" on page 526</li> <li>■ "<a href="#">Upgrading ClusterXL, VSX Cluster, or VRRP Cluster</a>" on page 538</li> <li>■ "<a href="#">Multi-Version Cluster Upgrade Procedure - Gateway Mode</a>" on page 581</li> <li>■ "<a href="#">Configuring a Single VSX Gateway in Monitor Mode</a>" on page 708</li> <li>■ Corrected the command to restart the Log Exporter</li> </ul>
06 April 2020	<p>Updated:</p> <ul style="list-style-type: none"> <li>■ "<a href="#">Backing Up and Restoring a Domain</a>" on page 635</li> <li>■ "<a href="#">Upgrade Methods</a>" on page 175 - added the description of the detailed upgrade report</li> <li>■ "<a href="#">Migrating Database from an R80.40 Security Management Server to an R80.40 Domain Management Server</a>" on page 643</li> <li>■ "<a href="#">Migrating Database from an R80.40 Domain Management Server to an R80.40 Security Management Server</a>" on page 647</li> </ul>

Date	Description
10 February 2020	Updated: <ul style="list-style-type: none"><li>■ <a href="#">"Contract Verification" on page 181</a></li><li>■ <a href="#">"Working with Licenses" on page 791</a></li><li>■ <a href="#">"Using Legacy SmartUpdate" on page 801</a></li></ul>
04 February 2020	Updated: <ul style="list-style-type: none"><li>■ <a href="#">"Migrating Database from an R80.40 Security Management Server to an R80.40 Domain Management Server" on page 643</a></li><li>■ <a href="#">"Migrating Database from an R80.40 Domain Management Server to an R80.40 Security Management Server" on page 647</a></li></ul>
03 February 2020	Updated: <ul style="list-style-type: none"><li>■ <a href="#">"Installing Software Packages on Gaia" on page 160</a> - added the description of the detailed upgrade report in Gaia Portal</li></ul>
30 January 2020	Added: <ul style="list-style-type: none"><li>■ <a href="#">"Migrating Database from an R80.40 Security Management Server to an R80.40 Domain Management Server" on page 643</a></li><li>■ <a href="#">"Migrating Database from an R80.40 Domain Management Server to an R80.40 Security Management Server" on page 647</a></li></ul> Updated: <ul style="list-style-type: none"><li>■ <a href="#">"Multi-Version Cluster Limitations" on page 578</a> - added the limitation "In a VSX Cluster, it is possible to install policy <b>only</b> on the <i>upgraded</i> VSX Cluster Members that run R80.40"</li></ul>
26 January 2020	First release of this document

# Table of Contents

---

<b>Glossary</b>	14
<b>Getting Started</b>	24
Welcome	24
R80.40 Documentation	24
R80.40 Software Images	24
For New Check Point Customers	24
Disk Space	25
Product Deployment Scenarios	25
<b>Backing Up and Restoring</b>	27
<b>The Gaia Operating System</b>	30
Installing the Gaia Operating System on Check Point Appliances	31
Installing the Gaia Operating System on Open Servers	33
Installing a Blink Image to Configure a Check Point Gateway Appliance	35
Changing Disk Partition Sizes During the Installation of Gaia Operating System	36
Running an Unattended USB Installation of Gaia on Check Point Appliances	37
Configuring Gaia for the First Time	38
Running the First Time Configuration Wizard in Gaia Portal	39
Running the First Time Configuration Wizard in CLI Expert mode	48
Configuring the IP Address of the Gaia Management Interface	56
Changing the Disk Partition Sizes on an Installed Gaia	58
Enabling IPv6 on Gaia	59
<b>Installing a Security Management Server</b>	61
Installing One Security Management Server only, or Primary Security Management Server in Management High Availability	62
Installing a Secondary Security Management Server in Management High Availability	64
<b>Installing a Dedicated Log Server or SmartEvent Server</b>	67
<b>Installing a Multi-Domain Server</b>	70
Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability	71
Installing a Secondary Multi-Domain Server in Management High Availability	72
<b>Installing a Multi-Domain Log Server</b>	74
<b>Installing an Endpoint Server</b>	76
Installing an Endpoint Security Management Server	77

---

---

Installing a Secondary Endpoint Security Management Server in Management High Availability .....	79
Installing an Endpoint Policy Server .....	82
Connection Port to Services on an Endpoint Security Management Server .....	84
Disk Space on an Endpoint Security Management Server .....	85
<b>Installing a CloudGuard Controller .....</b>	<b>86</b>
<b>Installing a Management Server on Linux .....</b>	<b>88</b>
<b>Installing SmartConsole .....</b>	<b>89</b>
Downloading SmartConsole .....	89
Installing SmartConsole .....	90
Logging in to SmartConsole .....	90
Troubleshooting SmartConsole .....	91
<b>Installing a Security Gateway, VSX Gateway .....</b>	<b>92</b>
Installing a Security Gateway .....	93
Installing a VSX Gateway .....	99
<b>Installing a ClusterXL, VSX Cluster, VRRP Cluster .....</b>	<b>104</b>
Installing a ClusterXL Cluster .....	105
Installing a VSX Cluster .....	123
Installing a VRRP Cluster .....	129
Full High Availability Cluster on Check Point Appliances .....	143
Understanding Full High Availability Cluster on Appliances .....	144
Installing Full High Availability Cluster .....	145
Recommended Logging Options for a Full High Availability Cluster .....	149
<b>Installing a Standalone .....</b>	<b>150</b>
<b>Post-Installation Configuration .....</b>	<b>154</b>
<b>Installing Software Packages on Gaia .....</b>	<b>160</b>
<b>Upgrade Options and Prerequisites .....</b>	<b>163</b>
Prerequisites for Upgrading and Migrating of Management Servers and Log Servers .....	164
Prerequisites for Upgrading and Migrating of Security Gateways and Clusters .....	169
Prerequisites for Upgrading the Mobile Access Software Blade Configuration .....	172
Prerequisites for Upgrading vSEC Controller R80.10 and lower .....	174
Upgrade Methods .....	175
Contract Verification .....	181
Management Server Migration Tool and Upgrade Tools .....	182
<b>Upgrade of Security Management Servers and Log Servers .....</b>	<b>185</b>
Upgrading a Security Management Server or vSEC Controller from R80.10 and lower .....	186

---

---

Upgrading a Security Management Server from R80.10 and lower with CPUSE .....	187
Upgrading a Security Management Server from R80.10 and lower with Advanced Upgrade .....	190
Upgrading a Security Management Server from R80.10 and lower with Migration .....	200
Upgrading Security Management Servers in Management High Availability from R80.10 and lower .....	207
Upgrading a Dedicated Log Server from R80.10 and lower .....	212
Upgrading a Dedicated Log Server from R80.10 and lower with CPUSE .....	213
Upgrading a Dedicated Log Server from R80.10 and lower with Advanced Upgrade .....	216
Upgrading a Dedicated Log Server from R80.10 and lower with Migration .....	222
Upgrading a Dedicated SmartEvent Server from R80.10 and lower .....	228
Upgrading a Dedicated SmartEvent Server from R80.10 and lower with CPUSE .....	229
Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Advanced Upgrade .....	232
Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Migration .....	238
Upgrading a Security Management Server or Log Server from R80.20 and higher .....	244
Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE .....	245
Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade .....	250
Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration .....	259
Upgrading Security Management Servers in Management High Availability from R80.20 and higher .....	268
<b>Upgrade of Multi-Domain Servers and Multi-Domain Log Servers .....</b>	<b>271</b>
Upgrading one Multi-Domain Server from R80.10 and lower .....	272
Upgrading one Multi-Domain Server from R80.10 and lower with CPUSE .....	273
Upgrading one Multi-Domain Server from R80.10 and lower with Advanced Upgrade .....	277
Upgrading one Multi-Domain Server from R80.10 and lower with Migration .....	285
Upgrading one R7x Multi-Domain Server with Gradual Migration of Domain Management Servers .....	293
Upgrading one Multi-Domain Server from R80.20 and higher .....	305
Upgrading one Multi-Domain Server from R80.20 and higher with CPUSE .....	306
Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade .....	309
Upgrading one Multi-Domain Server from R80.20 and higher with Migration .....	316
Upgrading Multi-Domain Servers in High Availability from R80.10 and lower .....	323
Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with CPUSE .....	324
Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Advanced Upgrade .....	329
Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Migration .....	343
Managing Domain Management Servers During the Upgrade Process .....	357

---

---

Upgrading Multi-Domain Servers in High Availability from R80.20 and higher .....	358
Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with CPUSE .....	359
Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade .....	366
Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration .....	387
Managing Domain Management Servers During the Upgrade Process .....	408
Upgrading a Multi-Domain Log Server from R80.10 and lower .....	409
Upgrading a Multi-Domain Log Server from R80.10 and lower with CPUSE .....	410
Upgrading a Multi-Domain Log Server from R80.10 and lower with Advanced Upgrade .....	414
Upgrading a Multi-Domain Log Server from R80.10 and lower with Migration .....	422
Upgrading a Multi-Domain Log Server from R80.20 and higher .....	430
Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE .....	431
Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade .....	437
Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration .....	446
<b>Upgrade of Endpoint Security Management Servers and Endpoint Policy Servers .....</b>	<b>455</b>
Upgrading an Endpoint Security Management Server from R80.10 and lower .....	456
Upgrading an Endpoint Security Management Server from R80.10 and lower with CPUSE .....	457
Upgrading an Endpoint Security Management Server from R80.10 and lower with Advanced Upgrade .....	460
Upgrading an Endpoint Security Management Server from R80.10 and lower with Migration .....	470
Upgrading Endpoint Security Management Servers in Management High Availability from R80.10 and lower .....	477
Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower .....	482
Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with CPUSE .....	483
Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Advanced Upgrade .....	487
Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Migration .....	493
Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher .....	499
Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE .....	500
Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade .....	505
Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration .....	513
Upgrading Endpoint Security Management Servers in Management High Availability from R80.20 and higher .....	522
<b>Upgrade of Security Gateways and Clusters .....</b>	<b>525</b>
Upgrading a Security Gateway or VSX Gateway .....	526

---

---

Upgrading a Security Gateway with CPUSE .....	527
Upgrading a VSX Gateway with CPUSE .....	531
Upgrading ClusterXL, VSX Cluster, or VRRP Cluster .....	538
Planning a Cluster Upgrade .....	539
Minimal Effort Upgrade .....	544
Minimal Effort Upgrade of a Security Gateway Cluster .....	545
Minimal Effort Upgrade of a VSX Cluster .....	549
Zero Downtime Upgrade .....	555
Zero Downtime Upgrade of a Security Gateway Cluster .....	556
Zero Downtime Upgrade of a VSX Cluster .....	564
Multi-Version Cluster (MVC) Upgrade .....	576
Multi-Version Cluster Upgrade Prerequisites .....	576
Supported Versions in Multi-Version Cluster .....	577
Multi-Version Cluster Limitations .....	578
General limitations in Multi-Version Cluster configuration .....	578
Limitations during failover in Multi-Version Cluster .....	580
Multi-Version Cluster Upgrade Procedure - Gateway Mode .....	581
Multi-Version Cluster Upgrade Procedure - VSX Mode .....	596
Troubleshooting the Multi-Version Cluster .....	615
Upgrading a Full High Availability Cluster .....	616
<b>Upgrading a Standalone from R80.10, R77.30 and lower .....</b>	<b>617</b>
Upgrading a Standalone from R80.10 and lower with CPUSE .....	618
Upgrading a Standalone from R80.10 and lower with Advanced Upgrade .....	621
Upgrading a Standalone from R80.10 and lower with Migration .....	628
<b>Special Scenarios for Management Servers .....</b>	<b>634</b>
Backing Up and Restoring a Domain .....	635
Migrating a Domain Management Server between R80.40 Multi-Domain Servers .....	637
Migrating Database Between R80.40 Security Management Servers .....	639
Migrating Database from an R80.40 Security Management Server to an R80.40 Domain Management Server .....	643
Migrating Database from an R80.40 Domain Management Server to an R80.40 Security Management Server .....	647
Migrating Global Policies from an R7x Multi-Domain Server .....	652
Migrating Database from an R7x Security Management Server to an R80.40 Domain Management Server .....	657
Migrating Database from an R7x Domain Management Server to an R80.40 Domain Management Server .....	663

---

---

Migrating Database from an R7x Standalone to an R80.40 Domain Management Server .....	670
Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server .....	681
Changing the IP Address of a Domain Management Server or Domain Log Server .....	687
IPS in Multi-Domain Server Environment .....	691
<b>Special Scenarios for Security Gateways .....</b>	<b>692</b>
Deploying a Security Gateway in Monitor Mode .....	693
Introduction to Monitor Mode .....	693
Example Topology for Monitor Mode .....	694
Supported Software Blades in Monitor Mode .....	694
Limitations in Monitor Mode .....	696
Configuring a Single Security Gateway in Monitor Mode .....	697
Configuring a Single VSX Gateway in Monitor Mode .....	708
Configuring Specific Software Blades for Monitor Mode .....	719
Configuring the Threat Prevention Software Blades for Monitor Mode .....	720
Configuring the Application Control and URL Filtering Software Blades for Monitor Mode .....	722
Configuring the Data Loss Prevention Software Blade for Monitor Mode .....	723
Configuring the Security Gateway in Monitor Mode Behind a Proxy Server .....	725
Deploying a Security Gateway or a ClusterXL in Bridge Mode .....	726
Introduction to Bridge Mode .....	726
Supported Software Blades in Bridge Mode .....	726
Limitations in Bridge Mode .....	728
Configuring a Single Security Gateway in Bridge Mode .....	729
Configuring a ClusterXL in Bridge Mode .....	737
Configuring ClusterXL in Bridge Mode - Active / Standby with Two Switches .....	738
Configuring ClusterXL in Bridge Mode - Active / Active with Two or Four Switches .....	752
Accept, or Drop Ethernet Frames with Specific Protocols .....	772
Routing and Bridge Interfaces .....	773
Managing a Security Gateway through the Bridge Interface .....	774
IPv6 Neighbor Discovery .....	776
Managing Ethernet Protocols .....	776
Configuring Link State Propagation (LSP) .....	779
Security Before Firewall Activation .....	783
Boot Security .....	784
The Initial Policy .....	789
Troubleshooting: Cannot Complete Reboot .....	790

---

---

<b>Working with Licenses</b>	<b>791</b>
Viewing Licenses in SmartConsole	792
Monitoring Licenses in SmartConsole	794
Managing Licenses in the Gaia Portal	798
Migrating a License to a New IP Address	799
<b>Using Legacy SmartUpdate</b>	<b>801</b>
Accessing SmartUpdate	802
Licenses Stored in the Licenses & Contracts Repository	803
Licensing Terms for SmartUpdate	804
Viewing the Licenses & Contracts Repository	806
Adding New Licenses to the Licenses & Contracts Repository	807
Deleting a License from the Licenses & Contracts Repository	809
Attaching a License to a Security Gateway	810
Detaching a License from a Security Gateway	811
Getting Licenses from Security Gateways	812
Exporting a License to a File	813
Checking for Expired Licenses	814
<b>Check Point Cloud Services</b>	<b>815</b>
Automatic Downloads	815
Sending Data to Check Point	817

# Glossary

## A

---

**Administrator**

A user with permissions to manage Check Point security products and the network environment.

**API**

In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components.

**Appliance**

A physical computer manufactured and distributed by Check Point.

## B

---

**Bond**

A virtual interface that contains (enslaves) two or more physical interfaces for redundancy and load sharing. The physical interfaces share one IP address and one MAC address. See "Link Aggregation".

**Bonding**

See "Link Aggregation".

**Bridge Mode**

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

## C

---

### CA

**Certificate Authority.** Issues certificates to gateways, users, or computers, to identify itself to connecting entities with Distinguished Name, public key, and sometimes IP address. After certificate validation, entities can send encrypted data using the public keys in the certificates.

### Certificate

An electronic document that uses a digital signature to bind a cryptographic public key to a specific identity. The identity can be an individual, organization, or software entity. The certificate is used to authenticate one identity to another.

### CGNAT

**Carrier Grade NAT.** Extending the traditional Hide NAT solution, CGNAT uses improved port allocation techniques and a more efficient method for logging. A CGNAT rule defines a range of original source IP addresses and a range of translated IP addresses. Each IP address in the original range is automatically allocated a range of translated source ports, based on the number of original IP addresses and the size of the translated range. CGNAT port allocation is Stateless and is performed during policy installation. See sk120296.

### Clean Install

Installation of a Check Point Operating System from scratch on a computer.

### Cluster

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

### Cluster Member

A Security Gateway that is part of a cluster.

### CoreXL

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

**CoreXL Firewall Instance**

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

**CoreXL SND**

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

**CPUSE**

Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. For details, see sk92449.

**D**

---

**DAIP Gateway**

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

**Data Type**

A classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

**Database**

The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

**Database Migration**

Process of: (1) Installing the latest Security Management Server or Multi-Domain Server version from the distribution media on a separate computer from the existing Security Management Server or Multi-Domain Server (2) Exporting the management database from the existing Security Management Server or Multi-Domain Server (3) Importing the management database to the new Security Management Server or Multi-Domain Server This upgrade method minimizes upgrade risks for an existing deployment.

**Distributed Deployment**

The Check Point Security Gateway and Security Management Server products are deployed on different computers.

**Domain**

A network or a collection of networks related to an entity, such as a company, business unit or geographical location.

**Domain Log Server**

A Log Server for a specified Domain, as part of a Multi-Domain Log Server. It stores and processes logs from Security Gateways that are managed by the corresponding Domain Management Server. Acronym: DLS.

---

**E****Expert Mode**

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

**External Network**

Computers and networks that are outside of the protected network.

**External Users**

Users defined on external servers. External users are not defined in the Security Management Server database or on an LDAP server. External user profiles tell the system how to identify and authenticate externally defined users.

## F

---

### **Firewall**

The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

### **Full High Availability Cluster**

Deployment and configuration mode of two Check Point appliances running Gaia OS. Each appliance runs both a Security Gateway and a Security Management Server software. The Security Gateways work as ClusterXL in High Availability mode. The Security Management Servers work in Management High Availability mode (see sk39345).

## 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 restrictive shell (role-based administration controls the number of commands available in the shell).

### **Gaia Portal**

Web interface for Check Point Gaia operating system.

## H

---

### **Hotfix**

A piece of software installed on top of the current software in order to fix some wrong or undesired behavior.

## I

---

### **ICA**

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

**Internal Network**

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

**IPv4**

Internet Protocol Version 4 (see RFC 791). A 32-bit number - 4 sets of numbers, each set can be from 0 - 255. For example, 192.168.2.1.

**IPv6**

Internet Protocol Version 6 (see RFC 2460 and RFC 3513). 128-bit number - 8 sets of hexadecimal numbers, each set can be from 0 - ffff. For example, FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

**J**

---

**Jumbo Hotfix Accumulator**

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

**L**

---

**Link Aggregation**

Technology that joins (aggregates) multiple physical interfaces together into one virtual interface, known as a bond interface. Also known as Interface Bonding, or Interface Teaming. This increases throughput beyond what a single connection could sustain, and provides redundancy in case one of the links should fail.

**Log**

A record of an action that is done by a Software Blade.

**Log Server**

A dedicated Check Point computer that runs Check Point software to store and process logs in Security Management Server or Multi-Domain Security Management environment.

## M

---

**Management High Availability**

Deployment and configuration mode of two Check Point Management Servers, in which they automatically synchronize the management databases with each other. In this mode, one Management Server is Active, and the other is Standby. Acronyms: Management HA, MGMT HA.

**Management Interface**

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

**Management Server**

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

**Migration**

Exporting the Check Point configuration database from one Check Point computer and importing it on another Check Point computer.

**Multi-Domain Log Server**

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

**Multi-Domain Security Management**

A centralized management solution for large-scale, distributed environments with many different Domain networks.

**Multi-Domain Server**

A computer that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Acronym: MDS.

## N

---

**Network Object**

Logical representation of every part of corporate topology (physical machine, software component, IP Address range, service, and so on).

**O**

---

**Open Server**

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

**P**

---

**Package Repository**

A SmartUpdate repository on the Security Management Server that stores uploaded packages. These packages are then used by SmartUpdate to perform upgrades of Check Point Small Office Appliances.

**R**

---

**Rule**

A set of traffic parameters and other conditions in a Rule Base that cause specified actions to be taken for a communication session.

**Rule Base**

Also Rulebase. All rules configured in a given Security Policy.

**S**

---

**SecureXL**

Check Point product that accelerates IPv4 and IPv6 traffic. Installed on Security Gateways for significant performance improvements.

**Security Gateway**

A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

**Security Management Server**

A computer that runs Check Point software to manage the objects and policies in Check Point environment.

**Security Policy**

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

**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 Sign-On**

A property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers. Acronym: SSO.

**SmartConsole**

A Check Point GUI application used to manage Security Policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

**SmartDashboard**

A legacy Check Point GUI client used to create and manage the security settings in R77.30 and lower versions.

**SmartUpdate**

A legacy Check Point GUI client used to manage licenses and contracts.

**Software Blade**

A software blade is a security solution based on specific business needs. Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

**SSO**

See "Single Sign-On".

**Standalone**

A Check Point computer, on which both the Security Gateway and Security Management Server products are installed and configured.

**T**

---

**Traffic**

Flow of data between network devices.

**U**

---

**Upgrade**

Replacing a Check Point product with a newer version of the same Check Point product.

**Users**

Personnel authorized to use network resources and applications.

**V**

---

**VLAN**

Virtual Local Area Network. Open servers or appliances connected to a virtual network, which are not physically connected to the same network.

**VLAN Trunk**

A connection between two switches that contains multiple VLANs.

**VSX**

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

**VSX Gateway**

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

# Getting Started

**Important** - Before you install or upgrade to R80.40:



1. Read the [R80.40 Release Notes](#).
2. Back up the current system. See ["Backing Up and Restoring" on page 27](#).

## Welcome

Thank you for choosing Check Point Software Blades for your security solution. We hope that you will be satisfied with this solution and our support services. Check Point products provide your business with the most up to date and secure solutions available today.

Check Point also delivers worldwide technical services including educational, professional, and support services through a network of Authorized Training Centers, Certified Support Partners, and Check Point technical support personnel to ensure that you get the most out of your security investment.

For additional information on the Internet Security Product Suite and other security solutions, go to <https://www.checkpoint.com> or call Check Point at 1(800) 429-4391.

For additional technical information, visit the [Check Point Support Center](#).

Welcome to the Check Point family. We look forward to meeting all of your current and future network, application, and management security needs.

## R80.40 Documentation

This guide is for administrators responsible for installing R80.40 on appliances and open servers that run the Gaia Operating System.

To learn what is new in R80.40, see the [R80.40 Release Notes](#).

See the [R80.40 Home Page SK](#) for information about the R80.40 release.

## R80.40 Software Images

You can use the [Upgrade/Download Wizard](#) to download the applicable installation and upgrade images.

## For New Check Point Customers

New Check Point customers can access the [Check Point User Center](#) to:

- Manage users and accounts
- Activate products
- Get support offers
- Open service requests
- Search the Technical Knowledge Base

# Disk Space

When you install or upgrade R80.40, the installation or upgrade wizard makes sure that there is sufficient space on the hard disk to install the Check Point products.

If there is not sufficient space on the hard disk, an error message is shown. The message states:

- The amount of disk space necessary to install the product.
- The directory where the product is installed.
- The amount of free disk space that is available in the directory.

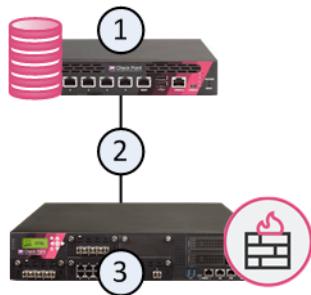
After there is sufficient disk space, install or upgrade the Check Point product.

# Product Deployment Scenarios

There are different deployment scenarios for Check Point software products.

## Distributed Deployment

The Security Management Server (1) and the Security Gateway (3) are installed on different computers, with a network connection (2).



## Standalone Deployment

The Security Management Server (1) and the Security Gateway (3) are installed on the same computer (2).



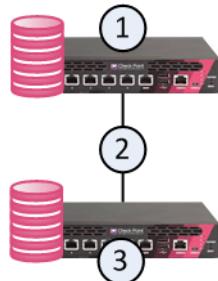
## Management High Availability

A Primary Security Management Server (1) has a direct or indirect connection (2) to a Secondary Security Management Server (3).

The databases of the Security Management Servers are synchronized, manually or on a schedule, to back up one another.

The administrator makes one Security Management Server Active and the others Standby.

If the Active Security Management Server is down, the administrator can promote the Standby server to be Active.



## Full High Availability

In a Full High Availability Cluster on two Check Point Appliances, each appliance runs both as a ClusterXL Cluster Member and as a Security Management Server, in High Availability mode.



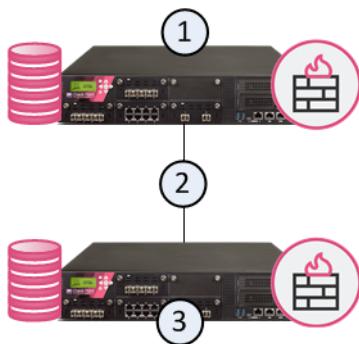
**Important** - You can deploy and configure a Full High Availability Cluster only on Check Point Appliances that support Standalone configuration. See the [R80.40 Release Notes](#) and "[Installing a Standalone](#)" on page 150.

This deployment reduces the maintenance required for your systems.

In the image below, the appliances are denoted as (1) and (3).

The two appliances are connected with a direct synchronization connection (2) and work in High Availability mode:

- The Security Management Server on one appliance (for example, 1) runs as Primary, and the Security Management Server on the other appliance (3) runs as Secondary.
- The ClusterXL on one appliance (for example, 1) runs as Active, and the ClusterXL on the other appliance (3), runs as Standby.
- The ClusterXL Cluster Members synchronize the information about the traffic over the synchronization connection (2).



# Backing Up and Restoring

## Best Practices:

Step	Instructions
1	<p>Before the upgrade:</p> <ul style="list-style-type: none"> <li>■ Save a snapshot of your source system. This backs up the entire configuration.</li> <li>■ Save a backup of your source system. This file lets you extract the most important configuration easily.</li> <li>■ Collect the <b>CPinfo</b> file from your source system (see <a href="#">sk92739</a>). This file lets you see the most important configuration easily with the <b>DiagnosticsView</b> tool (see <a href="#">sk125092</a>).</li> </ul>
2	<p>Immediately after the Pre-Upgrade Verifier (PUV) finishes successfully and does not show you further suggestions:</p> <ul style="list-style-type: none"> <li>■ Save a second snapshot of your source system.</li> <li>■ Save a second backup of your source system.</li> <li>■ Collect a second <b>CPinfo</b> file from your source system.</li> </ul>
3	<p>Transfer the CPinfo file, snapshot, backup files, and exported database files to external storage devices. Make sure to transfer the files in the binary mode.</p>

## Backing up and restoring in Management High Availability environment:

- To back up and restore a consistent Management High Availability environment, make sure to collect and restore the backups and snapshots from all Security Management Servers or Multi-Domain Security Management Servers at the same time. (This does **not** apply to Multi-Domain Log Servers.)
- Make sure other administrators do **not** make changes in SmartConsole until the backup operation is completed.

For more information:

- About Gaia Backup and Gaia Snapshot, see the [R80.40 Gaia Administration Guide](#).
- About the `migrate export` and `migrate import` commands, see the [R80.40 CLI Reference Guide](#).
- About the `mds_backup` and `mds_restore` commands, see the [R80.40 Multi-Domain Security Management Administration Guide](#).
- About Virtual Machine Snapshots, see the vendor documentation.

For more information, see:

1. [sk108902: Best Practices - Backup on Gaia OS](#)
2. *Gaia Administration Guide* (see the *Documentation* section in the Home Page SK for your current version)
3. [sk54100: How to back up your system on SecurePlatform](#)
4. *SecurePlatform Administration Guide* (see the *Documentation* section in the Home Page SK for your current version)
5. *Multi-Domain Security Management Administration Guide* (see the *Documentation* section in the Home Page SK for your current version) - Chapter *Command Line Reference* - Section *mds\_backup*
6. *Command Line Interface Reference Guide* - the `migrate` command.
7. [sk110173: How to migrate the events database from SmartEvent server R7x to SmartEvent Server R80 and above.](#)
8. [sk100395: How to backup and restore VSX Gateway.](#)
9. [sk127653: How to backup and restore Log Exporter configuration on R80.X upgrades.](#)

To back up a Security Management Server:

Operating System	Backup Recommendations
Gaia	<ol style="list-style-type: none"> <li>1. Take the Gaia snapshot.</li> <li>2. Collect the backup with the <code>"migrate export"</code> command.</li> </ol>
SecurePlatform	<ol style="list-style-type: none"> <li>1. Take the SecurePlatform snapshot.</li> <li>2. Collect the backup with the <code>migrate export</code> command.</li> </ol>
Linux	Collect the backup with the <code>migrate export</code> command.
Windows	Collect the backup with the <code>migrate export</code> command.

To back up a Multi-Domain Server:

Operating System	Backup Recommendations
Gaia	<ol style="list-style-type: none"> <li>1. Take the Gaia snapshot.</li> <li>2. Collect the full backup with the <code>mds_backup</code> command.</li> </ol>
SecurePlatform	<ol style="list-style-type: none"> <li>1. Take the SecurePlatform snapshot.</li> <li>2. Collect the full backup with the <code>mds_backup</code> command.</li> </ol>
Linux	Collect the full backup with the <code>mds_backup</code> command.

To back up a Security Gateway or a Cluster Member:

Operating System	Backup Recommendations
Gaia	Take the Gaia snapshot.
SecurePlatform	Take the SecurePlatform snapshot.

To back up a VSX environment:

Follow [sk100395: How to backup and restore VSX Gateway](#).

# The Gaia Operating System

This section provides instructions to install the Gaia Operating System and perform its initial configuration:

- "[Installing the Gaia Operating System on Check Point Appliances](#)" on page 31
- "[Installing the Gaia Operating System on Open Servers](#)" on page 33
- "[Installing a Blink Image to Configure a Check Point Gateway Appliance](#)" on page 35
- "[Changing Disk Partition Sizes During the Installation of Gaia Operating System](#)" on page 36
- "[Running an Unattended USB Installation of Gaia on Check Point Appliances](#)" on page 37
- "[Configuring Gaia for the First Time](#)" on page 38
- "[Configuring the IP Address of the Gaia Management Interface](#)" on page 56
- "[Changing the Disk Partition Sizes on an Installed Gaia](#)" on page 58
- "[Enabling IPv6 on Gaia](#)" on page 59

# Installing the Gaia Operating System on Check Point Appliances



**Note** - These instructions do not apply to the Check Point appliance models that run Gaia Embedded operating system.

For a list of supported appliances, see the [R80.40 Release Notes](#).

To install a clean Gaia Operating System on a Check Point appliance, these options are available:

## Reset a Check Point appliance to factory defaults



**Important** - This operation reverts the appliance to the last Gaia version that was installed using the Clean Install method.

Step	Instructions
1	Connect to the appliance using the serial console.
2	Restart the appliance.
3	During boot, when prompted, press any key within 4 seconds to enter the Boot menu: Loading the system Press any key to see the boot menu [Booting in 5 seconds]
4	Select <b>Reset to factory defaults</b> and press Enter.
5	Type <b>yes</b> and press Enter.
6	Run the Gaia First Time Configuration Wizard. See " <a href="#">Configuring Gaia for the First Time</a> " on page 38.

## Clean install with a Bootable USB device

Step	Instructions
1	Download the Gaia Operating System Clean Install ISO file from the R80.40 Home Page SK.
2	See <a href="#">sk65205</a> to create a bootable USB device.  <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <b>Important</b> - Always use the latest available build of the ISOmorphic Tool. If you use an outdated build, the installation can fail.         </div> </div>
3	Run the Gaia First Time Configuration Wizard. See " <a href="#">Configuring Gaia for the First Time</a> " on page 38.

## Clean install with the CPUSE

This option is available if Gaia is already installed.

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan for the local installation.

# Installing the Gaia Operating System on Open Servers

To install a clean Gaia Operating System on an Open Server, these options are available:

## Clean Install with a DVD-ROM

Step	Instructions
1	Download the Gaia Operating System Clean Install ISO file from the R80.40 Home Page SK.
2	Burn the ISO image onto a DVD disc.
3	Connect the DVD-ROM to your Open Server.
4	Reboot your Open Server.
5	Enter the BIOS and configure the DVD-ROM to be the first boot option.
6	Reboot your Open Server.
7	Your Open Server should boot from the DVD-ROM.
8	Gaia installation menu should appear.
9	Follow the instructions on the screen.
10	After Gaia installs and before the reboot, disconnect the DVD-ROM from your Open Server.
11	Reboot your Open Server.
12	Enter the BIOS and configure the Hard Disk to be the first boot option.
13	Reboot your Open Server.
14	Your Open Server should boot the Gaia operating system.
15	Run the Gaia First Time Configuration Wizard. See " <a href="#">Configuring Gaia for the First Time</a> " on page 38.

## Clean Install with a bootable USB device

To prepare a Bootable USB device, see [sk65205](#).

Step	Instructions
1	Download the Gaia Operating System ISO file from R80.40 Home Page SK.
2	See <a href="#">sk65205</a> to create a bootable USB device.  <b>Important</b> - Always use the latest available build of the ISOmorphic Tool. If you use an outdated build, the installation can fail.
3	Run the Gaia First Time Configuration Wizard. See " <a href="#">Configuring Gaia for the First Time</a> " on page 38.

## Clean Install with the CPUSE

This option is available if Gaia is already installed.

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan for the local installation.

# Installing a Blink Image to Configure a Check Point Gateway Appliance

*Blink* is a Gaia fast deployment procedure. With Blink utility, you can quickly deploy clean Check Point Security Gateways on appliances that have not yet been configured with the First Time Configuration Wizard. Blink deploys within 5-7 minutes.

When Blink utility completes the installation, clean Security Gateways, Hotfixes, and updated Software Blade signatures are installed. Blink utility configures an appliance automatically in place of the manual execution of the Gaia First Time Configuration Wizard.

You can run the Blink Gaia image from a USB or download it to your appliance.



**Note** - If you add the Blink image to a USB and insert the USB into the appliance before the First Time Configuration Wizard shows, the process begins automatically.

After the installation is complete, connect with your web browser to the Check Point appliance to complete the simplified Blink configuration.

In addition, the Blink utility lets you use a special XML file to run an unattended installation with predefined parameters for an appliance:

- Host name
- Gaia administrator password
- Network options - IP address, Subnet, Default Gateway
- Secure Internal Communication (SIC) key
- Cluster membership
- Upload to Check Point approval
- Download from Check Point approval

For complete information, see [sk120193](#).

# Changing Disk Partition Sizes During the Installation of Gaia Operating System

On Check Point appliances, the size of the disk partitions is predefined.

On these appliances, you can modify the default disk partitions within the first 20 seconds. If you miss this window, the non-interactive installation then continues:

- Smart-1 525, Smart-1 5050, and Smart-1 5150
- Smart-1 50, Smart-1 150, Smart-1 3050, and Smart-1 3150

When installing Gaia on an Open Server, these partitions have default sizes:

- System-swap
- System-root
- Logs
- Backup and upgrade

You can change the sizes of the *system-root* and the *logs* partitions. The storage size assigned for *backup and upgrade* partitions is updated accordingly.

To change the partition size, see [sk95566](#).

# Running an Unattended USB Installation of Gaia on Check Point Appliances

You can install a Gaia Operating System on Check Point appliances using an ISO on a removable USB drive (see [sk65205](#)).



**Important** - Always use the latest available build of the ISOmorphic Tool. If you use an outdated build, the installation can fail.

On Check Point appliances, the ISOmorphic tool lets an administrator run an *unattended* installation.

In an unattended installation, an experienced Check Point system administrator:

Step	Instructions
1	<p>Prepares the USB with these pre-configured settings for a specified network interface:</p> <ul style="list-style-type: none"> <li>■ IP address</li> <li>■ Network mask</li> <li>■ Default Gateway</li> </ul>
2	<p>Sends the USB drive to an administrator, who inserts the drive into the appliance and reboots it.</p> <p>The tool installs the Check Point Gaia OS and configures the appliance with the predefined settings.</p> <p>The LCD indicates a successful installation and interfaces blink in round-robin fashion.</p>
3	<p>The first administrator then:</p> <ul style="list-style-type: none"> <li>■ Connects to the Gaia Portal and runs the First Time Configuration Wizard, or</li> <li>■ Opens a command line to the appliance for further operating system level configuration</li> </ul>



**Note** - The ISOmorphic tool does **not** support unattended installation on Open Servers.

# Configuring Gaia for the First Time

After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

You can run the First Time Configuration Wizard in:

- Gaia Portal
- CLI Expert mode

# Running the First Time Configuration Wizard in Gaia Portal

To start the Gaia First Time Configuration Wizard:

Step	Instructions
1	Connect a computer to the Gaia computer. You must connect to the interface you configured during the Gaia installation (for example, <b>eth0</b> ).
2	On your connected computer, configure a static IPv4 address in the same subnet as the IPv4 address you configured during the Gaia installation.
3	On your connected computer, in a web browser, connect to the IPv4 address you configured during the Gaia installation:  <code>https://&lt;IP address of Gaia Management Interface&gt;</code>
4	Enter the default username and password: <b>admin</b> and <b>admin</b> .
5	Click <b>Login</b> . The Check Point <b>First Time Configuration Wizard</b> opens.
6	Follow the instructions on the First Time Configuration Wizard windows. See the applicable chapters below for installing specific Check Point products.

Below you can find the description of the First Time Configuration Wizard windows and their fields.

## Deployment Options window

In this window, you select how to deploy Gaia Operating System.

Section	Options	Description
Setup	<b>Continue with R80.40 configuration</b>	Use this option to configure the installed Gaia and Check Point products.
Install	<b>Install from Check Point Cloud</b> <b>Install from USB device</b>	Use these options to install a Gaia version.
Recovery	<b>Import existing snapshot</b>	Use this option to import an existing Gaia snapshot.

If in the **Deployment Options** window, you selected **Install from Check Point Cloud**, the First Time Configuration Wizard asks you to configure the connection to Check Point Cloud. These options appear (applies only to Check Point appliances that you configured as a Security Gateway):

- **Install major version** - This option let you choose and install major versions available on Check Point Cloud. The Gaia CPUSE performs the installation.
- **Pull appliance configuration** - This option applies the initial deployment configuration that includes different OS version on the appliance. You must prepare the initial deployment configuration with the Zero Touch Cloud Service. For more information, see [sk116375](#).

## 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 session.

Field	Description
<b>Interface</b>	By default, First Time Configuration Wizard selects the interface you configured during the Gaia installation (for example, <b>eth0</b> ).   <b>Note</b> - After you complete the First Time Configuration Wizard and reboot, you can select another interface as the main Gaia Management Interface and configure its IP settings.
<b>Configure IPv4</b>	Select how the Gaia Management Interface gets its IPv4 address: <ul style="list-style-type: none"> <li>■ <b>Manually</b> - You configure the IPv4 settings in the next fields.</li> <li>■ <b>Off</b> - None.</li> </ul>
<b>IPv4 address</b>	Enter the applicable IPv4 address.
<b>Subnet mask</b>	Enter the applicable IPv4 subnet mask.
<b>Default Gateway</b>	Enter the IPv4 address of the applicable default gateway.
<b>Configure IPv6</b>	Select how the Gaia Management Interface gets its IPv6 address: <ul style="list-style-type: none"> <li>■ <b>Manually</b> - You configure the IPv6 settings in the next fields.</li> <li>■ <b>Off</b> - None.</li> </ul>
<b>IPv6 Address</b>	Enter the applicable IPv6 address.
<b>Mask Length</b>	Enter the applicable IPv6 mask length.
<b>Default Gateway</b>	Enter the IPv6 address of the applicable default gateway.

## Internet Connection window

**Optional:** In this window, you configure the interface that connects the Gaia computer to the Internet.

<b>Interface</b>	Select the applicable interface on this computer.
<b>Configure IPv4</b>	Select how the applicable interface gets its IPv4 address: <ul style="list-style-type: none"> <li>■ <b>Manually</b> - You configure the IPv4 settings in the next fields.</li> <li>■ <b>Off</b> - None.</li> </ul>
<b>IPv4 address</b>	Enter the applicable IPv4 address.
<b>Subnet mask</b>	Enter the applicable IPv4 subnet mask.
<b>Configure IPv6</b>	Optional. Select how the applicable interface gets its IPv6 address: <ul style="list-style-type: none"> <li>■ <b>Manually</b> - You configure the IPv6 settings in the next fields.</li> <li>■ <b>Off</b> - None.</li> </ul>
<b>IPv6 Address</b>	Enter the applicable IPv6 address.
<b>Subnet</b>	Enter the applicable IPv6 subnet mask.

## Device Information window

In this window, you configure the Host name, the DNS servers and the Proxy server on the Gaia computer.

Field	Description
<b>Host Name</b>	Enter the applicable distinct host name.
<b>Domain Name</b>	Optional: Enter the applicable domain name.
<b>Primary DNS Server</b>	Enter the applicable IPv4 address of the primary DNS server.
<b>Secondary DNS Server</b>	Optional: Enter the applicable IPv4 address of the secondary DNS server.
<b>Tertiary DNS Server</b>	Optional: Enter the applicable IPv4 address of the tertiary DNS server.
<b>Use a Proxy server</b>	Optional: Select this option to configure the applicable Proxy server.
<b>Address</b>	Enter the applicable IPv4 address or resolvable hostname of the Proxy server.
<b>Port</b>	Enter the port number for the Proxy server.

## Date and Time Settings window

In this window, you configure the date and time settings on the Gaia computer.

Field	Description
<b>Set the time manually</b>	Select this option to configure the date and time settings manually.
<b>Date</b>	Select the correct date.
<b>Time</b>	Select the correct time.
<b>Time Zone</b>	Select the correct time zone.
<b>Use Network Time Protocol (NTP)</b>	Select this option to configure the date and time settings automatically with NTP.
<b>Primary NTP server</b>	Enter the applicable IPv4 address or resolvable hostname of the primary NTP server.
<b>Version</b>	Select the version of the NTP for the primary NTP server.
<b>Secondary NTP server</b>	Optional: Enter the applicable IPv4 address or resolvable hostname of the secondary NTP server.
<b>Version</b>	Select the version of the NTP for the secondary NTP server.
<b>Time Zone</b>	Select the correct time zone.

## Installation Type window

In this window, you select which type of Check Point products you wish to install on the Gaia computer.

Field	Description
<b>Security Gateway and/or Security Management</b>	Select this option to install: <ul style="list-style-type: none"> <li>■ A Single Security Gateway.</li> <li>■ A Cluster Member.</li> <li>■ A Security Management Server, including Management High Availability.</li> <li>■ An Endpoint Security Management Server.</li> <li>■ An Endpoint Policy Server.</li> <li>■ CloudGuard Controller.</li> <li>■ A dedicated single Log Server.</li> <li>■ A dedicated single SmartEvent Server.</li> <li>■ A Standalone.</li> </ul>
<b>Multi-Domain Server</b>	Select this option to install: <ul style="list-style-type: none"> <li>■ A Multi-Domain Server, including Management High Availability.</li> <li>■ A dedicated single Multi-Domain Log Server.</li> </ul>

## Products window

In this window, you continue to select which type of Check Point products you wish to install on the Gaia computer.

- If in the **Installation Type** window, you selected **Security Gateway and/or Security Management**, these options appear:

Field	Description
<b>Security Gateway</b>	Select this option to install: <ul style="list-style-type: none"> <li>A single Security Gateway.</li> <li>A Cluster Member.</li> <li>A Standalone.</li> </ul>
<b>Security Management</b>	Select this option to install: <ul style="list-style-type: none"> <li>A Security Management Server, including Management High Availability.</li> <li>An Endpoint Security Management Server.</li> <li>An Endpoint Policy Server.</li> <li>CloudGuard Controller.</li> <li>A dedicated single Log Server.</li> <li>A dedicated single SmartEvent Server.</li> <li>A Standalone.</li> </ul>
<b>Unit is a part of a cluster</b>	This option is available only if you selected <b>Security Gateway</b> . Select this option to install a cluster of dedicated Security Gateways, or a Full High Availability Cluster. Select the cluster type: <ul style="list-style-type: none"> <li><b>ClusterXL</b> - For a cluster of dedicated Security Gateways, or a Full High Availability Cluster.</li> <li><b>VRRP Cluster</b> - For a VRRP Cluster on Gaia.</li> </ul>
<b>Define Security Management as</b>	Select <b>Primary</b> to install: <ul style="list-style-type: none"> <li>A Security Management Server.</li> <li>An Endpoint Security Management Server.</li> <li>An Endpoint Policy Server.</li> <li>CloudGuard Controller.</li> </ul> Select <b>Secondary</b> to install: <ul style="list-style-type: none"> <li>A Secondary Management Server in Management High Availability.</li> </ul> Select <b>Log Server / SmartEvent only</b> to install: <ul style="list-style-type: none"> <li>A dedicated single Log Server.</li> <li>A dedicated single SmartEvent Server.</li> </ul>

- If in the **Installation Type** window, you selected **Multi-Domain Server**, these options appear:

Field	Description
<b>Primary Multi-Domain Server</b>	Select this option to install a Primary Multi-Domain Server in Management High Availability.

Field	Description
<b>Secondary Multi-Domain Server</b>	Select this option to install a Secondary Multi-Domain Server in Management High Availability.
<b>Multi-Domain Log Server</b>	Select this option to install a dedicated single Multi-Domain Log Server.



**Note** - By default, the option **Automatically download Blade Contracts, new software, and other important data** is enabled. See [sk111080](#).

### Dynamically Assigned IP window

In this window, you select if this Security Gateway gets its IP address dynamically (DAIP gateway).

Field	Description
<b>Yes</b>	Select this option, if this Security Gateway gets its IP address dynamically (DAIP gateway).
<b>No</b>	Select this option, if you wish to configure this Security Gateway with a static IP address.

### Secure Internal Communication (SIC) window

In this window, you configure a one-time Activation Key. You must enter this key later in SmartConsole when you create the corresponding object and initialize SIC.

Field	Description
<b>Activation Key</b>	Enter one-time activation key (between 4 and 127 characters long).
<b>Confirm Activation Key</b>	Enter the same one-time activation key again.

### Security Management Administrator window

In this window, you configure the main administrator for this Security Management Server.

<b>Use Gaia administrator: admin</b>	Select this option, if you wish to use the default Gaia administrator (admin).
<b>Define a new administrator</b>	Select this option, if you wish to configure an administrator username and password manually.

## Security Management GUI Clients window

In this window, you configure which computers are allowed to connect with SmartConsole to this Security Management Server.

Field	Description
<b>Any IP Address</b>	Select this option to allow all computers to connect.
<b>This machine</b>	Select this option to allow only a specific computer to connect. By default, the First Time Configuration Wizard uses the IPv4 address of your computer. You can change it to another IP address.
<b>Network</b>	Select this option to allow an entire IPv4 subnet of computers to connect. Enter the applicable subnet IPv4 address and subnet mask.
<b>Range of IPv4 addresses</b>	Select this option to allow a specific range of IPv4 addresses to connect. Enter the applicable start and end IPv4 addresses.

## Leading VIP Interfaces Configuration window

In this window, you select the main Leading VIP Interface on this Multi-Domain Server.

Field	Description
<b>Select leading interface</b>	Select the applicable interface.

## Multi-Domain Server GUI Clients window

In this window, you configure which computers are allowed to connect with SmartConsole to this Multi-Domain Server.

Field	Description
<b>Any host</b>	Select this option to allow all computers to connect.
<b>IP address</b>	Select this option to allow only a specific computer to connect. By default, the First Time Configuration Wizard uses the IPv4 address of your computer. You can change it to another IP address.

## First Time Configuration Wizard Summary window

In this window, you can see the installation options you selected.

The **Improve product experience** section:

- By default, the option **Send data to Check Point** is enabled. For information about this option, see [sk111080](#).
- By default, the option **Send crash data to Check Point that might contain personal data** is disabled.

If you enable this option, Gaia operating system uploads the detected core dump files to Check Point Cloud.

Check Point R&D can analyze the crashes and issue fixes for them.



### Notes:

- At the end of the First Time Configuration Wizard, the Gaia computer reboots and the initialization process is performed in the background for several minutes.
- If you installed the Gaia computer as a Security Management Server or Multi-Domain Server, only read-only access is possible with SmartConsole during this initialization time.
- To make sure the configuration is finished:
  1. Connect to the command line on the Gaia computer.
  2. Log in to the Expert mode.
  3. Check that the bottom section of the `/var/log/ftw_install.log` file contains one of these sentences:
    - `installation succeeded`
    - `FTW: Complete`

Run:

```
cat /var/log/ftw_install.log | egrep --color "installation succeeded|FTW: Complete"
```

**Example outputs:**

- From a Security Gateway or Cluster Member:

```
[Expert@GW:0]# cat /var/log/ftw_install.log | egrep --color "installation succeeded|FTW: Complete"
Dec 06, 19 19:19:51 FTW: Complete
[Expert@GW:0]#
```

- From a Security Management Server or a Standalone:

```
[Expert@SA:0]# cat /var/log/ftw_install.log | egrep --color "installation succeeded|FTW: Complete"
Dec 06, 2019 03:48:38 PM installation succeeded.
06/12/19 15:48:39 FTW: Complete
[Expert@SA:0]#
```

- From a Multi-Domain Server:

```
[Expert@MDS:0]# cat /var/log/ftw_install.log | egrep --color "installation succeeded|FTW: Complete"
Dec 06, 2019 07:43:15 PM installation succeeded.
[Expert@MDS:0]#
```

# Running the First Time Configuration Wizard in CLI Expert mode

## Description

Use this command in the Expert mode to test and to run the First Time Configuration Wizard on a Gaia system for the first time after the system installation.

### Notes:



- The `config_system` utility is **not** an interactive configuration tool. It helps automate the first time configuration process.
- The `config_system` utility is only for the first time configuration, and **not** for ongoing system configurations.

## Syntax

- To list the command options, run one of these:

Form	Command
Short form	<code>config_system -h</code>
Long form	<code>config_system --help</code>

- To run the First Time Configuration Wizard from a specified configuration file, run one of these:

Form	Command
Short form	<code>config_system -f &lt;Path and Filename&gt;</code>
Long form	<code>config_system --config-file &lt;Path and Filename&gt;</code>

- To run the First Time Configuration Wizard from a specified configuration string, run one of these:

Form	Command
Short form	<code>config_system -s &lt;String&gt;</code>
Long form	<code>config_system --config-string &lt;String&gt;</code>

- To create a First Time Configuration Wizard Configuration file template in a specified path, run one of these:

Form	Command
Short form	<code>config_system -t &lt;Path&gt;</code>
Long form	<code>config_system --create-template &lt;Path&gt;</code>

- To verify that the First Time Configuration file is valid, run:

```
config_system --dry-run
```

- To list configurable parameters, run one of these:

Form	Command
Short form	config_system -l
Long form	config_system --list-params

#### To run the First Time Configuration Wizard from a configuration string:

Step	Instructions
1	<p>Run this command in Expert mode:</p> <pre>config_system --config-string &lt;String of Parameters and Values&gt;</pre> <p>A configuration string must consist of <i>parameter=value</i> pairs, separated by the ampersand (&amp;). You must enclose the whole string between quotation marks.</p> <p>For example:</p> <pre>"hostname=myhost&amp;domainname=somedomain.com&amp;timezone='America/Indianapolis'&amp;ftw_sic_key=aaaa&amp;install_security_gw=true&amp;gateway_daip=false&amp;install_ppak=true&amp;gateway_cluster_member=true&amp;install_security_managment=false"</pre> <p>For more information on valid parameters and values, run the "config_system -h" command.</p>
2	Reboot the system.

#### To run the First Time Configuration Wizard from a configuration file:

Step	Instructions
1	<p>Run this command in Expert mode:</p> <pre>config_system -f &lt;FileName&gt;</pre>
2	Reboot the system.

If you do not have a configuration file, you can create a configuration template and fill in the parameter values as necessary.

Before you run the First Time Configuration Wizard, you can validate the configuration file you created.

**To create a configuration file:**

Step	Instructions
1	Run this command in Expert mode: <pre>config_system -t &lt;File Name&gt;</pre>
2	Open the file you created in a text editor.
3	Edit all parameter values as necessary.
4	Save the updated configuration file.

**To validate a configuration file:**

Run this command in Expert mode:

```
config_system --config-file <File Name> --dry-run
```

**Parameters**

A configuration file contains the `<parameter>=<value>` pairs described in the table below.



**Note** - The `config_system` parameters can change from Gaia version to Gaia version. Run the "`config_system --help`" command to see the available parameters.

Table: The 'config\_system' parameters

Parameter	Description	Valid values
<code>install_security_gw</code>	Installs Security Gateway, if its value is set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>
<code>gateway_daip</code>	Configures the Security Gateway as Dynamic IP (DAIP) Security Gateway, if its value is set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>  <p><b>Note</b> - Must be set to "false", if ClusterXL or Security Management Server is enabled.</p>
<code>gateway_cluster_member</code>	Configures the Security Gateway as member of ClusterXL, if its value is set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>
<code>install_security_management</code>	Installs Security Management Server, if its value is set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>

Table: The 'config\_system' parameters (continued)

Parameter	Description	Valid values
install_mgmt_primary	Makes the installed Security Management Server the Primary one.   <b>Note</b> - The value of the "install_security_managment" parameter must be set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>  <b>Note</b> - Can only be set to "true", if the value of the "install_mgmt_secondary" parameter is set to "false".
install_mgmt_secondary	Makes the installed Security Management Server a Secondary one.   <b>Note</b> - The value of the "install_security_managment" parameter must be set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>  <b>Note</b> - Can only be set to "true", if the value of the "install_mgmt_primary" parameter is set to "false".
install_mds_primary	Makes the installed Security Management Server the Primary Multi-Domain Server.   <b>Note</b> - The value of the "install_security_managment" parameter must be set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>  <b>Note</b> - Can only be set to "true", if the value of the "install_mds_secondary" parameter is set to "false".
install_mds_secondary	Makes the installed Security Management Server a Secondary Multi-Domain Server.   <b>Note</b> - The value of the "install_security_managment" parameter must be set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>  <b>Note</b> - Can only be set to "true", if the value of the "install_mds_primary" parameter is set to "false".
install_mlm	Installs Multi-Domain Log Server, if its value is set to "true".	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>
install_mds_interface	Specifies Multi-Domain Server management interface.	Name of the interface exactly as it appears in the device configuration. Examples: eth0, eth1

Table: The 'config\_system' parameters (continued)

Parameter	Description	Valid values
download_info	<p>Downloads Check Point Software Blade contracts and other important information, if its value is set to "true".</p> <p>For more information, see <a href="#">sk94508</a>.</p> <p> <b>Best Practice</b> - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>
upload_info	<p>Uploads data that helps Check Point provide you with optimal services, if its value is set to "true".</p> <p>For more information, see <a href="#">sk94509</a>.</p> <p> <b>Best Practice</b> - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>
mgmt_admin_radio	<p>Configures Management Server administrator.</p> <p> <b>Note</b> - You must specify this parameter, if you install a Management Server.</p>	<ul style="list-style-type: none"> <li>■ Set the value to "gaia_admin", if you wish to use the Gaia "admin" account.</li> <li>■ Set the value to "new_admin", if you wish to configure a new administrator account.</li> </ul>
mgmt_admin_name	<p>Configures the management administrator's username.</p> <p> <b>Note</b> - You must specify this parameter, if the value of the "install_security_managment" parameter is set to "true".</p>	A string of alphanumeric characters.
mgmt_admin_passwd	<p>Configures the management administrator's password.</p> <p> <b>Note</b> - You must specify this parameter, if the value of the "install_security_managment" parameter is set to "true".</p>	A string of alphanumeric characters.
mgmt_gui_clients_radio	Specifies SmartConsole clients that can connect to the Security Management Server.	<ul style="list-style-type: none"> <li>■ any</li> <li>■ range</li> <li>■ network</li> <li>■ this</li> </ul>
mgmt_gui_clients_first_ip_field	Specifies the first address of the range, if the value of the "mgmt_gui_clients_radio" parameter is set to "range".	Single IPv4 address of a host. Example: 192.168.0.10

Table: The 'config\_system' parameters (continued)

Parameter	Description	Valid values
mgmt_gui_clients_last_ip_field	Specifies the last address of the range, if the value of the "mgmt_gui_clients_radio" parameter is set to "range".	Single IPv4 address of a host. Example: 192.168.0.20
mgmt_gui_clients_ip_field	Specifies the network address, if the value of the "mgmt_gui_clients_radio" parameter is set to "network".	IPv4 address of a network. Example: 192.168.0.0
mgmt_gui_clients_subnet_field	Specifies the netmask, if the value of the "mgmt_gui_clients_radio" parameter is set to "network".	A number from 1 to 32.
mgmt_gui_clients_hostname	Specifies the netmask, if value of the "mgmt_gui_clients_radio" parameter is set to "this".	Single IPv4 address of a host. Example: 192.168.0.15
ftw_sic_key	Configures the Secure Internal Communication key, if the value of the "install_security_managment" parameter is set to "false".	A string of alphanumeric characters (between 4 and 127 characters long).
admin_hash	Configures the administrator's password.	A string of alphanumeric characters, enclosed between single quotation marks.
iface	Interface name (optional).	Name of the interface exactly as it appears in the device configuration. Examples: eth0, eth1
ipstat_v4	Turns on static IPv4 configuration, if its value is set to "manually".	<ul style="list-style-type: none"> <li>■ manually</li> <li>■ off</li> </ul>
ipaddr_v4	Configures the IPv4 address of the management interface.	Single IPv4 address.
masklen_v4	Configures the IPv4 mask length for the management interface.	A number from 0 to 32.
default_gw_v4	Specifies IPv4 address of the default gateway.	Single IPv4 address.
ipstat_v6	Turns static IPv6 configuration on, if its value is set to "manually".	<ul style="list-style-type: none"> <li>■ manually</li> <li>■ off</li> </ul>
ipaddr_v6	Configures the IPv6 address of the management interface.	Single IPv6 address.
masklen_v6	Configures the IPv6 mask length for the management interface.	A number from 0 to 128.

Table: The 'config\_system' parameters (continued)

Parameter	Description	Valid values
default_gw_v6	Specifies IPv6 address of the default gateway.	Single IPv6 address.
hostname	Configures the name of the local host (optional).	A string of alphanumeric characters.
domainname	Configures the domain name (optional).	Fully qualified domain name. <b>Example:</b> somedomain.com
timezone	Configures the Area/Region (optional).	The Area/Region must be enclosed between single quotation marks. <b>Examples:</b> 'America/New_York' 'Asia/Tokyo'  <b>Note</b> - To see the available Areas and Regions, connect to any Gaia computer, log in to Gaia Clish, and run this command (names of Areas and Regions are case-sensitive): set timezone Area <SPACE><TAB>
ntp_primary	Configures the IP address of the primary NTP server (optional).	IPv4 address.
ntp_primary_version	Configures the NTP version of the primary NTP server (optional).	<ul style="list-style-type: none"> <li>■ 1</li> <li>■ 2</li> <li>■ 3</li> <li>■ 4</li> </ul>
ntp_secondary	Configures the IP address of the secondary NTP server (optional).	IPv4 address.
ntp_secondary_version	Configures the NTP version of the secondary NTP server (optional).	<ul style="list-style-type: none"> <li>■ 1</li> <li>■ 2</li> <li>■ 3</li> <li>■ 4</li> </ul>
primary	Configures the IP address of the primary DNS server (optional).	IPv4 address.
secondary	Configures the IP address of the secondary DNS server (optional).	IPv4 address.

Table: The 'config\_system' parameters (continued)

Parameter	Description	Valid values
tertiary	Configures the IP address of the tertiary DNS server (optional).	IPv4 address.
proxy_address	Configures the IP address of the proxy server (optional).	IPv4 address, or Hostname.
proxy_port	Configures the port number of the proxy server (optional).	A number from 1 to 65535.
reboot_if_required	Reboots the system after the configuration, if its value is set to "true" (optional).	<ul style="list-style-type: none"> <li>■ true</li> <li>■ false</li> </ul>

# Configuring the IP Address of the Gaia Management Interface

The Gaia Management Interface is pre-configured with the IP address **192.168.1.1**.

You can change this IP address during or after you run the Gaia First Time Configuration Wizard.

If you must access the Gaia computer over the network, assign the applicable IP address to that interface before you connect the Gaia computer to the network.

If you change the IP address of the Gaia Management Interface during the First Time Configuration Wizard, this warning shows:

Your IP address has been changed. In order to maintain the browser connection, the old IP address will be retained as a secondary IP address.

You can change the IP address of the Gaia Management Interface after you run the Gaia First Time Configuration Wizard.

## Changing the IP address in Gaia Portal

Step	Instructions
1	In your web browser, connect the Gaia Portal to the current IP address of the Gaia management interface: <i>https://&lt;IP Address of Gaia Management Interface&gt;</i>
2	In the left navigation tree, go to <b>Network Management &gt; Network Interfaces</b> .
3	In the <b>Management Interface</b> section, click <b>Set Management Interface</b> .
4	Select the applicable interface.
5	Click <b>OK</b> .
6	In the <b>Interfaces</b> section, select the Management Interface and click <b>Edit</b> .
7	Assign the applicable IP address.
8	Click <b>OK</b> .

## Changing the IP address in Gaia Clish

Step	Instructions
1	<p>Connect to the command line on the Gaia computer.</p> <ul style="list-style-type: none"> <li>■ Over SSH to the current IP address of the Gaia Management Interface</li> <li>■ Over a console</li> </ul>
2	Log in to Gaia Clish.
3	<p>Get the name of the current Gaia Management Interface:</p> <pre>show management interface</pre>
4	<p>Select another Gaia Management Interface:</p> <pre>set management interface &lt;Interface Name&gt;</pre>
5	<p>Assign another IP address to the Gaia Management Interface:</p> <pre>set interface &lt;Interface Name&gt; ipv4-address &lt;IPv4 address&gt; subnet-mask &lt;Mask&gt;</pre>
6	<p>Save the changes in the Gaia database:</p> <pre>save config</pre>

### For more information:

See the [R80.40 Gaia Administration Guide](#).

# Changing the Disk Partition Sizes on an Installed Gaia

See the [R80.40 Release Notes](#) for disk space requirements.

To see the size of the system-root and log partitions on an installed system:

Step	Instructions
1	Connect to the command line on your Gaia computer.
2	Log in to the Expert mode.
3	Run: <code>df -h</code>



**Note** - Most of the remaining space on the disk is reserved for backup images and upgrades.

To see the disk space assigned for backup images:

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <code>https://&lt;IP address of Gaia Management Interface&gt;</code>
2	In the left navigation tree, click <b>Maintenance &gt; Snapshot Management</b> .  <b>Note</b> - On an Open Server, the available space in the <b>Snapshot Management</b> page is less than the space you defined during the Gaia installation. The difference is the space reserved for upgrades. The amount of reserved space equals the size of the <i>system-root</i> partition.

To manage the partition size on your system, see [sk95566](#).

# Enabling IPv6 on Gaia

IPv6 is automatically enabled, if you configure IPv6 addresses in the Gaia First Time Configuration Wizard.

If you did not configure IPv6 addresses, you can manually enable the IPv6 support in Gaia later.

## Enabling IPv6 in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at:  <code>https://&lt;IP address of Gaia Management Interface&gt;</code>
2	From the navigation tree, click <b>System Management &gt; System Configuration</b> .
3	In the <b>IPv6 Support</b> section, select <b>On</b> .
4	Click <b>Apply</b> .
5	When prompted, select <b>Yes</b> to reboot.   <b>Important</b> - IPv6 support is <b>not</b> available until you reboot.

## Enabling IPv6 in Gaia Clish

Step	Instructions
1	Connect to the command line on Gaia.
2	Log in to Gaia Clish.
3	Enable the IPv6 support:  <code>set ipv6-state on</code>
4	Save the changes:  <code>save config</code>
5	Reboot:  <code>reboot</code>   <b>Important</b> - IPv6 support is <b>not</b> available until you reboot.

**For more information:**

See the [\*R80.40 Gaia Administration Guide\*](#) > Chapter *System Management* > Section *System Configuration*.

# Installing a Security Management Server

This section provides instructions to install a Security Management Server:

- [\*"Installing One Security Management Server only, or Primary Security Management Server in Management High Availability" on page 62\*](#)
- [\*"Installing a Secondary Security Management Server in Management High Availability" on page 64\*](#)

# Installing One Security Management Server only, or Primary Security Management Server in Management High Availability

## Procedure:

### 1: Install the Security Management Server

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:             <ol style="list-style-type: none"> <li>1. In the <b>Products</b> section, select <b>Security Management</b> only.</li> <li>2. In the <b>Clustering</b> section, in the <b>Define Security Management as</b> field, select <b>Primary</b>.</li> </ol> </li> <li>■ In the <b>Security Management GUI Clients</b> window, configure the applicable allowed computers:             <ul style="list-style-type: none"> <li>• <b>Any IP Address</b> - Allows all computers to connect.</li> <li>• <b>This machine</b> - Allows only the single specified computer to connect.</li> <li>• <b>Network</b> - Allows all computers on the specified network to connect.</li> <li>• <b>Range of IPv4 addresses</b> - Allows all computers in the specified range to connect.</li> </ul> </li> </ul>
4	<p>Install a valid license. See <a href="#">"Working with Licenses" on page 791</a>.</p>

### 2: Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Security Management Server object.
4	On the <b>General Properties</b> page, click the <b>Management</b> tab.

Step	Instructions
5	<p>Enable the applicable Software Blades.</p>  <p><b>Note</b> - In a Management High Availability environment, the SmartEvent Software Blade is supported only on the <b>Active</b> Management Server (for more information, see <a href="#">sk25164</a>).</p>
6	Click <b>OK</b> .

#### Disk space for logs and indexes:

The Security Management Server with **Log Indexing** enabled, creates and uses index files for fast access to log file content. Index files are located by default at \$RTDIR/log\_indexes/.

To make sure that there is always sufficient disk space on the Security Management Server, the server that stores the log index deletes the oldest index entries, when the available disk space is less than a specified minimum. The default minimum value is 5000 MB, or 15% of the available disk space.

#### Configuring the applicable minimum disk space

Step	Instructions
1	In the SmartConsole, edit the object of the Security Management Server.
2	From the left navigation tree, click <b>Logs &gt; Storage</b> .
3	Select <b>When disk space is below &lt;number&gt; Mbytes, start deleting old files</b> .
4	Enter the applicable disk space value.
5	Click <b>OK</b> .

#### For more information:

See the [\*R80.40 Security Management Administration Guide\*](#).

# Installing a Secondary Security Management Server in Management High Availability

## Procedure:

### 1. Install the Secondary Security Management Server

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul> <p> <b>Important</b> - You must use the same Gaia installation version as you used for the Primary Security Management Server.</p>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:             <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Management</b> only.</li> <li>b. In the <b>Clustering</b> section, in the <b>Define Security Management as</b> field, select <b>Secondary</b>.</li> </ol> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	<p>Install a valid license.</p> <p>See <a href="#">"Working with Licenses" on page 791</a>.</p>

### 2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Primary Security Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new <b>Check Point Host</b> object that represents the Secondary Security Management Server in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★) &gt; More &gt; Check Point Host</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object &gt; Gateways &amp; Servers &gt; New Check Point Host</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Check Point Host</b>.</li> </ul>

Step	Instructions
4	Click the <b>General Properties</b> page.
5	In the <b>Name</b> field, enter the applicable name.
6	In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, enter the applicable IP addresses.
7	In the <b>Platform</b> section: <ul style="list-style-type: none"> <li>■ In the <b>Hardware</b> field, select the applicable option</li> <li>■ In the <b>Version</b> field, select <b>R80.40</b></li> <li>■ In the <b>OS</b> field, select <b>Gaia</b></li> </ul>
8	On the <b>General Properties</b> page, click the <b>Management</b> tab.
9	Select <b>Network Policy Management</b> . Make sure the <b>Secondary Server</b> is selected and grayed out.
 9	<b>Note</b> - In a Management High Availability environment, the SmartEvent Software Blade is supported only on the <b>Active Management Server</b> (for more information, see <a href="#">sk25164</a> ).
	10 Establish the Secure Internal Communication (SIC) between the Primary Security Management Server and the Secondary Security Management Server: <ol style="list-style-type: none"> <li>a. In the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>b. Enter the same Activation Key you entered during the First Time Configuration Wizard of the Secondary Security Management Server.</li> <li>c. Click <b>Initialize</b>. The <b>Trust state</b> field must show <b>Established</b>.</li> <li>d. Click <b>Close</b>.</li> </ol>
11	Click <b>OK</b> .
12	In the SmartConsole top left corner, click <b>Menu &gt; Install database</b> .
13	Select all objects.
14	Click <b>Install</b> .
15	Click <b>OK</b> .
16	In the SmartConsole top left corner, click <b>Menu &gt; Management High Availability</b> .
17	Make sure the Security Management Servers are able to synchronize.

**Disk space for logs and indexes:**

The Security Management Server with **Log Indexing** enabled, creates and uses index files for fast access to log file content. Index files are located by default at \$RTDIR/log\_indexes/.

To make sure that there is always sufficient disk space on the Security Management Server, the server that stores the log index deletes the oldest index entries, when the available disk space is less than a specified minimum. The default minimum value is 5000 MB, or 15% of the available disk space.

**Configuring the applicable minimum disk space**

Step	Instructions
1	In the SmartConsole, edit the object of the Security Management Server.
2	From the left navigation tree, click <b>Logs &gt; Storage</b> .
3	Select <b>When disk space is below &lt;number&gt; Mbytes, start deleting old files</b> .
4	Enter the applicable disk space value.
5	Click <b>OK</b> .

**For more information:**

See the [\*R80.40 Security Management Administration Guide\*](#).

# Installing a Dedicated Log Server or SmartEvent Server

## Procedure:

### 1. Install the Log Server or SmartEvent Server



**Note** - You can install a dedicated SmartEvent Server and a dedicated SmartEvent Correlation Unit.

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Management</b> only.</li> <li>b. In the <b>Clustering</b> section, in the <b>Define Security Management as</b> field, select <b>Log Server / SmartEvent only</b>.</li> </ol> </li> <li>■ In the <b>Security Management Administrator</b> window, select one of these options:               <ul style="list-style-type: none"> <li>• <b>Use Gaia administrator</b></li> <li>• <b>Define a new administrator</b> and configure it</li> </ul> </li> <li>■ In the <b>Security Management GUI Clients</b> window, configure the applicable allowed computers:               <ul style="list-style-type: none"> <li>• <b>Any IP Address</b> - Allows all computers to connect.</li> <li>• <b>This machine</b> - Allows only the single specified computer to connect.</li> <li>• <b>Network</b> - Allows all computers on the specified network to connect.</li> <li>• <b>Range of IPv4 addresses</b> - Allows all computers in the specified range to connect.</li> </ul> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791</a> .

### 2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server that works with this Log Server or SmartEvent Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new <b>Check Point Host</b> object that represents the dedicated Log Server or SmartEvent Server in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (*) &gt; More &gt; Check Point Host</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object &gt; Gateways &amp; Servers &gt; New Check Point Host</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Check Point Host</b>.</li> </ul>
4	Click the <b>General Properties</b> page.
5	In the <b>Name</b> field, enter the applicable name.
6	In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, enter the applicable IP addresses.
7	<p>In the <b>Platform</b> section:</p> <ul style="list-style-type: none"> <li>■ In the <b>Hardware</b> field, select the applicable option</li> <li>■ In the <b>Version</b> field, select <b>R80.40</b></li> <li>■ In the <b>OS</b> field, select <b>Gaia</b></li> </ul>
8	<p>On the <b>Management</b> tab, select the applicable Software Blades:</p> <ul style="list-style-type: none"> <li>■ For the Log Server, select: <ul style="list-style-type: none"> <li>• <b>Logging &amp; Status</b></li> <li>• <b>Identity Logging</b>, if you work with Identity Awareness Software Blade</li> </ul> </li> <li>■ For the SmartEvent Server, select: <ul style="list-style-type: none"> <li>• <b>SmartEvent Server</b></li> <li>• <b>SmartEvent Correlation Unit</b></li> </ul> <p>Note - You can install a dedicated SmartEvent Server and a dedicated SmartEvent Correlation Unit.</p> </li> </ul>
9	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this dedicated Log Server or SmartEvent Server:</p> <ol style="list-style-type: none"> <li>a. In the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>b. Enter the same Activation Key you entered during the First Time Configuration Wizard of the dedicated Log Server or SmartEvent Server.</li> <li>c. Click <b>Initialize</b>. The <b>Trust state</b> field must show <b>Established</b>.</li> <li>d. Click <b>Close</b>.</li> </ol>
10	In the left tree, configure the applicable settings.
11	Click <b>OK</b> .
12	In the SmartConsole top left corner, click <b>Menu &gt; Install database</b> .
13	Select all objects.

Step	Instructions
14	Click <b>Install</b> .
15	Click <b>OK</b> .

#### Disk space for logs and indexes:

The Log Server or SmartEvent Server with **Log Indexing** enabled, creates and uses index files for fast access to log file content. Index files are located by default at \$RTDIR/log\_indexes/.

To make sure that there is always sufficient disk space on the Log Server or SmartEvent Server, the server that stores the log index deletes the oldest index entries when the available disk space is less than a specified minimum. The default minimum value is 5000 MB, or 15% of the available disk space.

#### Configuring the applicable minimum disk space

Step	Instructions
1	In the SmartConsole, edit the object of the Security Management Server.
2	From the left navigation tree, click <b>Logs &gt; Storage</b> .
3	Select <b>When disk space is below &lt;number&gt; Mbytes, start deleting old files</b> .
4	Enter the applicable disk space value.
5	Click <b>OK</b> .



**Note** - In a Multi-Domain Security Management environment, the Multi-Domain Server controls the disk space for logs and indexes. The configured disk space applies to all Domain Management Servers. Configure the applicable disk space in the Multi-Domain Server object.

#### For more information, see the:

- [R80.40 Security Management Administration Guide](#)
- [R80.40 Logging and Monitoring Administration Guide](#)

# Installing a Multi-Domain Server

This section provides instructions to install a Multi-Domain Server:

- [\*"Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 71\*](#)
- [\*"Installing a Secondary Multi-Domain Server in Management High Availability" on page 72\*](#)

# Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability

## Procedure:

### 1. Install the Multi-Domain Server

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38.</a>
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Multi-Domain Server</b>.</li> <li>■ In the <b>Installation Type</b> window, select <b>Primary Multi-Domain Server</b>.</li> <li>■ In the <b>Leading VIP Interfaces Configuration</b> window, select the applicable interface.</li> <li>■ In the <b>Multi-Domain Server GUI Clients</b> window, select one of these options:               <ul style="list-style-type: none"> <li>• <b>Any host</b> to allow all computers to connect</li> <li>• <b>IP address</b> and enter the IPv4 address of the applicable allowed computer</li> </ul> </li> <li>■ In the <b>Security Management Administrator</b> window, select one of these options:               <ul style="list-style-type: none"> <li>• <b>Use Gaia administrator</b></li> <li>• <b>Define a new administrator</b> and configure it</li> </ul> </li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791.</a>

### 2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the <b>Multi-Domain Server</b> .
2	Configure the applicable settings.

## For more information:

See the [R80.40 Multi-Domain Security Management Administration Guide](#).

# Installing a Secondary Multi-Domain Server in Management High Availability

## Procedure:

### 1. Install the Secondary Multi-Domain Server

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul> <p> <b>Important</b> - You must use the same Gaia installation version as you used for the Primary Multi-Domain Server.</p>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Multi-Domain Server</b>.</li> <li>■ In the <b>Installation Type</b> window, select <b>Secondary Multi-Domain Server</b>.</li> <li>■ In the <b>Leading VIP Interfaces Configuration</b> window, select the applicable interface.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	<p>Install a valid license. See <a href="#">"Working with Licenses" on page 791</a>.</p>

### 2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Primary Multi-Domain Server - the <b>MDS</b> context.
2	From the left navigation panel, click <b>Multi Domain &gt; Domains</b> .
3	From the top toolbar, click <b>New &gt; Multi-Domain Server</b> .
4	Enter the applicable object name.
5	Click the <b>General</b> page.
6	<p>In the <b>Basic Details</b> section:</p> <ol style="list-style-type: none"> <li>Enter the applicable IPv4 address.</li> <li>Click <b>Connect</b>.</li> </ol>

Step	Instructions
7	Enter the same Activation Key you entered during the setup of First Time Configuration Wizard of the Secondary Multi-Domain Server.
8	Click <b>OK</b> .
7	In the <b>Platform</b> section: <ul style="list-style-type: none"> <li>■ In the <b>OS</b> field, select <b>Gaia</b></li> <li>■ In the <b>Version</b> field, select <b>R80.40</b></li> <li>■ In the <b>Hardware</b> field, select the applicable option</li> </ul>
8	Click the <b>Multi-Domain</b> page.
9	Configure the applicable settings.
10	Click the <b>Log Settings &gt; General</b> page.
11	Configure the applicable settings.
12	Click the <b>Log Settings &gt; Advanced Settings</b> page.
13	Configure the applicable settings.
14	Click <b>OK</b> .

**Notes:**

- The new Multi-Domain Server automatically synchronizes with all existing Multi-Domain Servers and Multi-Domain Log Servers. The synchronization operation can take some time to complete, during which a notification indicator shows in the task information area.
- It is **not** supported to move the Secondary Multi-Domain Server from one Management High Availability environment to another Management High Availability environment. If you disconnect the existing Secondary Multi-Domain Server from one Management High Availability environment and connect it to another, you must install it again from scratch as a Secondary Multi-Domain Server (Known Limitation PMTR-14327).

**For more information:**

See the [\*R80.40 Multi-Domain Security Management Administration Guide\*](#).

# Installing a Multi-Domain Log Server

## Procedure:

### 1. Install the Multi-Domain Log Server

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Multi-Domain Server</b>.</li> <li>■ In the <b>Installation Type</b> window, select <b>Multi-Domain Log Server</b>.</li> <li>■ In the <b>Leading VIP Interfaces Configuration</b> window, select the applicable interface.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791</a> .

### 2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Primary Multi-Domain Server - the <b>MDS</b> context.
2	From the left navigation panel, click <b>Multi Domain &gt; Domains</b> .
3	From the top toolbar, click <b>New &gt; Multi-Domain Log Server</b> .
4	Enter the applicable object name.
5	Click the <b>General</b> page.
6	In the <b>Basic Details</b> section: <ol style="list-style-type: none"> <li>a. Enter the applicable IPv4 address.</li> <li>b. Click <b>Connect</b>.</li> </ol>
7	Enter the same Activation Key you entered during the First Time Configuration Wizard of the Multi-Domain Log Server.
8	Click <b>OK</b> .

Step	Instructions
9	In the <b>Platform</b> section: <ul style="list-style-type: none"><li>■ In the <b>OS</b> field, select <b>Gaia</b></li><li>■ In the <b>Version</b> field, select <b>R80.40</b></li><li>■ In the <b>Hardware</b> field, select the applicable option</li></ul>
10	Click the <b>Multi-Domain</b> page.
11	Configure the applicable settings.
12	Click the <b>Log Settings &gt; General</b> page.
13	Configure the applicable settings.
14	Click the <b>Log Settings &gt; Advanced Settings</b> page.
15	Configure the applicable settings.
16	Click <b>OK</b> .

**For more information:**

See the [\*R80.40 Multi-Domain Security Management Administration Guide\*](#).

# Installing an Endpoint Server

This section describes the installation and basic configuration of Endpoint Security Management Server and Endpoint Policy Server:

- [\*"Installing an Endpoint Security Management Server" on page 77\*](#)
- [\*"Installing an Endpoint Policy Server" on page 82\*](#)
- [\*"Connection Port to Services on an Endpoint Security Management Server" on page 84\*](#)
- [\*"Disk Space on an Endpoint Security Management Server" on page 85\*](#)

# Installing an Endpoint Security Management Server

## Procedure:

### 1. Install the Endpoint Security Management Server

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:             <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Management</b> only.</li> <li>b. In the <b>Clustering</b> section, in the <b>Define Security Management as</b> field, select <b>Primary</b>.</li> </ol> </li> <li>■ In the <b>Security Management GUI Clients</b> window, configure the applicable allowed computers:             <ul style="list-style-type: none"> <li>• <b>Any IP Address</b> - Allows all computers to connect.</li> <li>• <b>This machine</b> - Allows only the single specified computer to connect.</li> <li>• <b>Network</b> - Allows all computers on the specified network to connect.</li> <li>• <b>Range of IPv4 addresses</b> - Allows all computers in the specified range to connect.</li> </ul> </li> </ul>
4	<p>Install a valid license. See <a href="#">"Working with Licenses" on page 791</a>.</p>

### 2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Security Management Server object.
4	On the <b>General Properties</b> page, click the <b>Management</b> tab.
5	Select the <b>Endpoint Policy Management</b> blade.
6	Click <b>OK</b> .

Step	Instructions
7	In the SmartConsole top left corner, click <b>Menu &gt; Install database</b> .
8	Select all objects.
9	Click <b>Install</b> .
10	Click <b>OK</b> .

**For more information:**

See the [\*R80.40 Endpoint Security Server Administration Guide\*](#).

# Installing a Secondary Endpoint Security Management Server in Management High Availability

## Procedure:

### 1. Install the Secondary Endpoint Security Management Server

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul> <p> <b>Important</b> - You must use the same Gaia installation version as you used for the Primary Endpoint Security Management Server.</p>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:             <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Management</b> only.</li> <li>b. In the <b>Clustering</b> section, in the <b>Define Security Management as</b> field, select <b>Secondary</b>.</li> </ol> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	<p>Install a valid license. See <a href="#">"Working with Licenses" on page 791</a>.</p>

### 2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Primary Endpoint Security Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	<p>Create a new <b>Check Point Host</b> object that represents the Secondary Endpoint Security Management Server in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★ &gt; More &gt; Check Point Host</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways &amp; Servers</b> &gt; <b>New Check Point Host</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Check Point Host</b>.</li> </ul>
4	Click the <b>General Properties</b> page.
5	In the <b>Name</b> field, enter the applicable name.
6	In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, enter the applicable IP addresses.
7	<p>In the <b>Platform</b> section:</p> <ul style="list-style-type: none"> <li>■ In the <b>Hardware</b> field, select the applicable option</li> <li>■ In the <b>Version</b> field, select <b>R80.40</b></li> <li>■ In the <b>OS</b> field, select <b>Gaia</b></li> </ul>
8	On the <b>General Properties</b> page, click the <b>Management</b> tab.
9	<p>Select the <b>Endpoint Policy Management</b> blade.</p>  <p><b>Note</b> - In a Management High Availability environment, the SmartEvent Software Blade is supported only on the <b>Active</b> Management Server (for more information, see <a href="#">sk25164</a>).</p>
10	<p>Establish the Secure Internal Communication (SIC) between the Primary Endpoint Security Management Server and the Secondary Endpoint Security Management Server:</p> <ol style="list-style-type: none"> <li>a. In the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>b. Enter the same Activation Key you entered during the First Time Configuration Wizard of the Secondary Endpoint Security Management Server.</li> <li>c. Click <b>Initialize</b>. The <b>Trust state</b> field must show <b>Established</b>.</li> <li>d. Click <b>Close</b>.</li> </ol>
11	Click <b>OK</b> .
12	In the SmartConsole top left corner, click <b>Menu &gt; Install database</b> .
13	Select all objects.
14	Click <b>Install</b> .
15	Click <b>OK</b> .
16	In the SmartConsole top left corner, click <b>Menu &gt; Management High Availability</b> .
17	Make sure the Endpoint Security Management Servers are able to synchronize.

**For more information:**

See the [\*R80.40 Endpoint Security Server Administration Guide\*](#).

# Installing an Endpoint Policy Server

## Procedure:

### 1. Install the dedicated Endpoint Security Management Server

Follow the instructions in "["Installing an Endpoint Security Management Server" on page 77.](#)

### 2. Install the dedicated Endpoint Policy Server

Follow the installation step instructions in "["Installing a Dedicated Log Server or SmartEvent Server" on page 67.](#)

### 3. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Endpoint Security Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new <b>Check Point Host</b> object that represents the Endpoint Policy Server in one of these ways: <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (*) &gt; More &gt; Check Point Host</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object &gt; Gateways &amp; Servers &gt; New Check Point Host</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Check Point Host</b>.</li> </ul>
4	Click the <b>General Properties</b> page.
5	In the <b>Name</b> field, enter the applicable name.
6	In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, enter the applicable IP addresses.
7	In the <b>Platform</b> section: <ul style="list-style-type: none"> <li>■ In the <b>Hardware</b> field, select the applicable option</li> <li>■ In the <b>Version</b> field, select <b>R80.40</b></li> <li>■ In the <b>OS</b> field, select <b>Gaia</b></li> </ul>
8	On the <b>Management</b> tab, select both the <b>Endpoint Policy Management</b> and <b>Logging &amp; Status</b> Software Blades.
9	Establish the Secure Internal Communication (SIC) between the Endpoint Security Management Server and the Endpoint Policy Server: <ol style="list-style-type: none"> <li>a. In the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>b. Enter the same Activation Key you entered during the First Time Configuration Wizard of this dedicated Log Server.</li> <li>c. Click <b>Initialize</b>. The <b>Trust state</b> field must show <b>Established</b>.</li> <li>d. Click <b>Close</b>.</li> </ol>

Step	Instructions
10	Click <b>OK</b> .
11	In the SmartConsole top left corner, click <b>Menu &gt; Install database</b> .
12	Select all objects.
13	Click <b>Install</b> .
14	Click <b>OK</b> .

**For more information:**

See the [\*R80.40 Endpoint Security Server Administration Guide\*](#).

# Connection Port to Services on an Endpoint Security Management Server

- When you enable the **Endpoint Policy Management** Software Blade on a Security Management Server, the SSL connection port to these services automatically changes from the default TCP port **443** to the TCP port **4434**:

- Gaia Portal

Configuration	URL and Port
Default	<code>https://&lt;IP Address of Gaia Management Interface&gt;</code>
New	<code>https://&lt;IP Address of Gaia Management Interface&gt;:4434</code>

- SmartView Web Application

Configuration	URL and Port
Default	<code>https://&lt;IP Address of Management Server&gt;/smartview/</code>
New	<code>https://&lt;IP Address of Management Server&gt;:4434/smartview/</code>

- Management API Web Services (see [Check Point Management API Reference](#))

Configuration	URL and Port
Default	<code>https://&lt;IP Address of Management Server&gt;/web_api/&lt;command&gt;</code>
New	<code>https://&lt;IP Address of Management Server&gt;:4434/web_api/&lt;command&gt;</code>

- When you disable the **Endpoint Policy Management** Software Blade on a Security Management Server, the SSL connection port automatically changes back to the default TCP port **443**.

# Disk Space on an Endpoint Security Management Server

We recommend that you have at least 10 GB available for Endpoint Security in the root partition.

Client packages and main release files are stored in the root partition:

Required Space	Instructions
4 GB	Main Security Management Server installation files.
2 GB or more	Client files (each additional version of client packages requires 1 GB of disk space).
1 GB	Logs.
1 GB	High Availability support (more can be required in large environments).



**Note** - To make future upgrades easier, we recommend that you use a larger disk size than necessary in this deployment.

# Installing a CloudGuard Controller



**Note** - See the Known Limitation VSECPC-1341 in the [R80.40 Known Limitations SK](#).

## Procedure:

### 1. Install the CloudGuard Controller

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Management</b> only.</li> <li>b. In the <b>Clustering</b> section, in the <b>Define Security Management as</b> field, select <b>Primary</b>.</li> </ol> </li> <li>■ In the <b>Security Management GUI Clients</b> window, configure the applicable allowed computers:               <ul style="list-style-type: none"> <li>• <b>Any IP Address</b> - Allows all computers to connect.</li> <li>• <b>This machine</b> - Allows only the single specified computer to connect.</li> <li>• <b>Network</b> - Allows all computers on the specified network to connect.</li> <li>• <b>Range of IPv4 addresses</b> - Allows all computers in the specified range to connect.</li> </ul> </li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791</a> .

### 2. Enable the CloudGuard Controller

Step	Instructions
1	Connect to the command line on the Security Management Server.
2	Log in to the Gaia Clish, or Expert mode.
3	Run: <div style="border: 1px solid black; padding: 5px; width: fit-content;">clouguard on</div>

### 3. Enable the Identity Awareness Software Blade

Enable the Identity Awareness Software Blade on the applicable Security Gateways.

For more information, see the:

- [\*R80.40 CloudGuard Controller Administration Guide\*](#)
- [\*R80.40 Identity Awareness Administration Guide\*](#)

# Installing a Management Server on Linux

To install a Security Management Server or Multi-Domain Server on Red Hat Enterprise Linux:

1. See [sk44925](#).
2. Follow [sk98760](#).
3. Contact [Check Point Support](#) for specific installation instructions.

# Installing SmartConsole

SmartConsole is a GUI client you use to manage the Check Point environment.

For SmartConsole requirements, see the [R80.40 Release Notes](#).

## Downloading SmartConsole

You can download the SmartConsole installation package in several ways:

### Downloading the SmartConsole package from the Home Page SK

Step	Instructions
1	Open the <a href="#">R80.40 Home Page SK</a> .
2	Go to the <b>Downloads</b> section.
3	Click the <b>SmartConsole</b> link.
4	Save the SmartConsole installation file.

### Downloading the SmartConsole package from the Support Center

Step	Instructions
1	Connect to the <a href="#">Check Point Support Center</a> .
2	Search for: "R80.40 SmartConsole"
3	Click the <b>Downloads</b> tab.
4	Click the applicable link to open the download page.
5	Click the <b>Download</b> button.
6	Save the SmartConsole installation file.

## Downloading the SmartConsole package from the Gaia Portal

You can download the SmartConsole package from the Gaia Portal of your Security Management Server or Multi-Domain Server.

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; width: fit-content;"> https://&lt;IP address of Gaia Management Interface&gt; </div>
2	On the <b>Overview</b> page, click <b>Download Now!</b>
3	Save the SmartConsole installation file.

## Installing SmartConsole

To install the SmartConsole client on Windows platforms:

Step	Instructions
1	Transfer the SmartConsole installation file to a Windows-based computer you wish to use as a SmartConsole Client.
2	Run the <b>SmartConsole</b> installation file with Administrator privileges.
3	Follow the instructions on the screen.

## Logging in to SmartConsole

Step	Instructions
1	Open the SmartConsole application.
2	Enter the IP address or resolvable hostname of the Security Management Server, Multi-Domain Server, or Domain Management Server. The Management Server authenticates the connection when you log in for the first time. Multiple administrators can log in at the same time.
3	Enter your administrator credentials, or select the certificate file.
4	Click <b>Login</b> .
5	If necessary, confirm the connection using the fingerprint generated during the installation. You see this only the first time that you log in from a SmartConsole client.

### For more information:

See the [R80.40 Security Management Administration Guide](#).

# Troubleshooting SmartConsole

Make sure the SmartConsole client can access these ports on the Management Server:

- 18190
- 18264
- 19009

For more information, see:

- [sk52421: Ports used by Check Point software](#)
- [sk43401: How to completely disable FireWall Implied Rules](#)

# Installing a Security Gateway, VSX Gateway

This section provides instructions to install a Security Gateway and a VSX Gateway:

- [\*"Installing a Security Gateway" on page 93\*](#)
- [\*"Installing a VSX Gateway" on page 99\*](#)

# Installing a Security Gateway

**Notes:**



- This procedure applies to both Check Point Appliances and Open Servers.
- This procedure does **not** apply to Check Point Small Office Appliance models lower than 3000.

**Procedure:**

1. **Install the Security Gateway**

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#"><i>"Installing the Gaia Operating System on Check Point Appliances" on page 31</i></a></li> <li>■ <a href="#"><i>"Installing the Gaia Operating System on Open Servers" on page 33</i></a></li> </ul>
2	Follow <a href="#"><i>"Configuring Gaia for the First Time" on page 38.</i></a>
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster, type</b>.</li> </ol> </li> <li>■ In the <b>Dynamically Assigned IP</b> window, select the applicable option.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	Install a valid license. See <a href="#"><i>"Working with Licenses" on page 791.</i></a>

2. **Configure the Security Gateway object in SmartConsole**

## ■ Configuring in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new Security Gateway object in one of these ways: <ul style="list-style-type: none"> <li>• From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>• In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>New Gateway</b>.</li> <li>• In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Gateway</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Creation</b> window, click <b>Wizard Mode</b> .
5	On the <b>General Properties</b> page: <ol style="list-style-type: none"> <li>a. In the <b>Gateway name</b> field, enter the applicable name for this Security Gateway object.</li> <li>b. In the <b>Gateway platform</b> field, select the correct hardware type.</li> <li>c. In the <b>Gateway IP address</b> section, select the applicable option:               <ul style="list-style-type: none"> <li>• If you selected <b>Static IP address</b>, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Gateway's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> <li>• If this Security Gateway receives its IP addresses from a DHCP server, click <b>Cancel</b> and follow the procedure <b>Step 2 of 3: Configure the Security Gateway object in SmartConsole - Classic Mode</b> below.</li> </ul> </li> <li>d. Click <b>Next</b>.</li> </ol>
6	On the <b>Trusted Communication</b> page: <ol style="list-style-type: none"> <li>a. Select the applicable option:               <ul style="list-style-type: none"> <li>• If you selected <b>Initiate trusted communication now</b>, enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>• If you selected <b>Skip and initiate trusted communication later</b>, make sure to follow Step 7.</li> </ul> </li> <li>b. Click <b>Next</b>.</li> </ol>
7	On the <b>End</b> page: <ol style="list-style-type: none"> <li>a. Examine the <b>Configuration Summary</b>.</li> <li>b. Select <b>Edit Gateway properties for further configuration</b>.</li> <li>c. Click <b>Finish</b>.</li> </ol> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>

Step	Instructions
8	<p>If during the Wizard Mode, you selected <b>Skip and initiate trusted communication later</b>:</p> <ol style="list-style-type: none"> <li>a. The <b>Secure Internal Communication</b> field shows Uninitialized.</li> <li>b. Click <b>Communication</b>.</li> <li>c. In the <b>Platform</b> field: <ul style="list-style-type: none"> <li>• Select <b>Open server / Appliance</b> for all Check Point appliance models 3000 and higher.</li> <li>• Select <b>Open server / Appliance</b> for an Open Server.</li> <li>• Select <b>Small Office Appliance</b> only for Check Point Small Office Appliance models lower than 3000.</li> </ul> </li> <li>d. Enter the same <b>Activation Key</b> you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>e. Click <b>Initialize</b>. Make sure the <b>Certificate state</b> field shows <b>Established</b>.</li> <li>f. Click <b>OK</b>.</li> </ol>
9	<p>On the <b>General Properties</b> page:</p> <ul style="list-style-type: none"> <li>• On the <b>Network Security</b> tab, enable the applicable Software Blades.</li> <li>• On the <b>Threat Prevention</b> tab, enable the applicable Software Blades.</li> </ul>
10	Click <b>OK</b> .
11	Publish the SmartConsole session.

## ■ Configuring in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>• From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>• In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>New Gateway</b>.</li> <li>• In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Gateway</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>.  <b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
5	In the <b>Name</b> field, enter the applicable name for this Security Gateway object.
6	<p>In the <b>IPv4 address</b> and <b>IPv6 address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Gateway's First Time Configuration Wizard.  Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.  If this Security Gateway receives its IP addresses from a DHCP server, select <b>Dynamic Address</b>.</p>
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:</p> <ol style="list-style-type: none"> <li>a. Near the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>b. In the <b>Platform</b> field: <ul style="list-style-type: none"> <li>• Select <b>Open server / Appliance</b> for all Check Point models 3000 and higher.</li> <li>• Select <b>Open server / Appliance</b> for an Open Server.</li> </ul> </li> <li>c. Enter the same <b>Activation Key</b> you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>d. Click <b>Initialize</b>.</li> <li>e. Click <b>OK</b>.</li> </ol>

Step	Instructions
	<p>If the <b>Certificate state</b> field does not show <b>Established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Gateway.</li> <li>Make sure there is a physical connectivity between the Security Gateway and the Management Server (for example, pings can pass).</li> <li>Run:  <pre>cpcconfig</pre> </li> <li>Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpcconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
8	<p>In the <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>In the <b>Hardware</b> field: <ul style="list-style-type: none"> <li>If you install the Security Gateway on a Check Point Appliance, select the correct appliances series.</li> <li>If you install the Security Gateway on an Open Server, select <b>Open server</b>.</li> </ul> </li> <li>In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
9	<p>Enable the applicable Software Blades:</p> <ul style="list-style-type: none"> <li>On the <b>Network Security</b> tab.</li> <li>On the <b>Threat Prevention</b> tab.</li> </ul>
10	<p>Click <b>OK</b>.</p>
11	<p>Publish the SmartConsole session.</p>

### 3. Configure the applicable Security Policy for the Security Gateway in SmartConsole

Step	Instructions
1	<p>Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Gateway.</p>
2	<p>From the left navigation panel, click <b>Security Policies</b>.</p>
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> <li>At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>Click <b>Close</b>.</li> <li>On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>

Step	Instructions
4	Create the applicable Access Control rules.
5	Install the Access Control Policy on the Security Gateway object.
6	Create the applicable Threat Prevention rules.
7	Install the Threat Prevention Policy on the Security Gateway object.

For more information, see the:

- [\*R80.40 Security Management Administration Guide\*](#)
- [\*R80.40 Threat Prevention Administration Guide\*](#)
- Applicable *Administration Guides* on the [\*R80.40 Home Page\*](#).

# Installing a VSX Gateway

## Notes:



- This procedure applies to both Check Point Appliances and Open Servers.
- This procedure does **not** apply to Check Point Small Office Appliance models lower than 3000.

## Procedure:

### 1. Install the VSX Gateway

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster, type</b>.</li> </ol> </li> <li>■ In the <b>Dynamically Assigned IP</b> window, select the applicable option.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791</a> .

### 2. Configure the VSX Gateway object in SmartConsole



- The steps below are only for a Clean Install of a new VSX Gateway. To configure a VSX Gateway that failed, see the [R80.40 VSX Administration Guide](#) > Chapter *Command Line Reference* > Section *vsx\_util* > Section *vsx\_util reconfigure*.
- The steps below are for the Dedicated Management Interfaces (DMI) configuration. For the non-DMI configuration, see the [R80.40 VSX Administration Guide](#).

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Main Domain Management Server</i> that should manage this VSX Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	<p>Create a new VSX Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★)</b> &gt; <b>VSX</b> &gt; <b>Gateway</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>VSX</b> &gt; <b>New Gateway</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>VSX</b> &gt; <b>Gateway</b>.</li> </ul> <p>The <b>VSX Gateway Wizard</b> opens.</p>
4	<p>On the <b>VSX Gateway General Properties (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>a. In the <b>Enter the VSX Gateway Name</b> field, enter the applicable name for this VSX Gateway object.</li> <li>b. In the <b>Enter the VSX Gateway IPv4</b> field, enter the same IPv4 address that you configured on the <b>Management Connection</b> page of the VSX Gateway's First Time Configuration Wizard.</li> <li>c. In the <b>Enter the VSX Gateway IPv6</b> field, enter the same IPv6 address that you configured on the <b>Management Connection</b> page of the VSX Gateway's First Time Configuration Wizard.</li> <li>d. In the <b>Select the VSX Gateway Version</b> field, select <b>R80.40</b>.</li> <li>e. Click <b>Next</b>.</li> </ol>
5	<p>On the <b>VSX Gateway General Properties (Secure Internal Communication)</b> page:</p> <ol style="list-style-type: none"> <li>a. In the <b>Activation Key</b> field, enter the same Activation Key you entered during the VSX Gateway's First Time Configuration Wizard.</li> <li>b. In the <b>Confirm Activation Key</b> field, enter the same Activation Key again.</li> <li>c. Click <b>Initialize</b>.</li> <li>d. Click <b>Next</b>.</li> </ol> <p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Make sure there is a physical connectivity between the VSX Gateway and the Management Server (for example, pings can pass).</li> <li>c. Run:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">cpconfig</div> <li>d. Enter the number of this option:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">Secure Internal Communication</div> <li>e. Follow the instructions on the screen to change the Activation Key.</li> <li>f. In SmartConsole, on the <b>VSX Gateway General Properties</b> page, click <b>Reset</b>.</li> <li>g. Enter the same Activation Key you entered in the <b>cpconfig</b> menu.</li> <li>h. In SmartConsole, click <b>Initialize</b>.</li> </ol>

Step	Instructions
6	<p>On the <b>VSX Gateway Interfaces (Physical Interfaces Usage)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway.</li> <li>If you plan to connect more than one Virtual System directly to the same physical interface, you must select <b>VLAN Trunk</b> for that physical interface.</li> <li>Click <b>Next</b>.</li> </ol>
7	<p>On the <b>Virtual Network Device Configuration (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>You can select <b>Create a Virtual Network Device</b> and configure the first applicable Virtual Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router.</li> <li>Click <b>Next</b>.</li> </ol>
8	<p>On the <b>VSX Gateway Management (Specify the management access rules)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the default access rules.</li> <li>Select the applicable default access rules.</li> <li>Configure the applicable source objects, if needed.</li> <li>Click <b>Next</b>.</li> </ol>
	<p><b>Important</b> - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.</p>
9	<p>On the <b>VSX Gateway Creation Finalization</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Finish</b> and wait for the operation to finish.</li> <li>Click <b>View Report</b> for more information.</li> <li>Click <b>Close</b>.</li> </ol>
10	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the VSX Gateway.</li> <li>Log in to the Expert mode.</li> <li>Run:</li> </ol> <pre data-bbox="520 1394 711 1423">vsx stat -v</pre>
11	<p>Open the VSX Gateway object.</p>
12	<p>On the <b>General Properties</b> page, click the <b>Network Security</b> tab.</p>
13	<p>Enable the applicable Software Blades for the VSX Gateway object itself (context of VS0).</p> <p>Refer to:</p> <ul style="list-style-type: none"> <li>■ <a href="#">sk79700: VSX supported features on R75.40VS and above</a></li> <li>■ <a href="#">sk106496: Software Blades updates on VSX R75.40VS and above - FAQ</a></li> <li>■ Applicable <i>Administration Guides</i> on the <a href="#">R80.40 Home Page</a>.</li> </ul>
14	<p>Click <b>OK</b> to push the updated VSX Configuration.</p> <p>Click <b>View Report</b> for more information.</p>

Step	Instructions
15	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 384 711 413">vsx stat -v</pre>
16	<p>Install the default policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> <li>a. Click <b>Install Policy</b>.</li> <li>b. In the <b>Policy</b> field, select the default policy for this VSX Gateway object. This policy is called:</li> </ol> <pre data-bbox="520 619 1060 649">&lt;Name of VSX Gateway object&gt;_VSX</pre> <ol style="list-style-type: none"> <li>c. Click <b>Install</b>.</li> </ol>
17	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 889 711 918">vsx stat -v</pre>
18	Configure the applicable Threat Prevention Policy for this VSX Gateway.
19	<p>Install the applicable Threat Prevention Policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> <li>a. Click <b>Install Policy</b>.</li> <li>b. In the <b>Policy</b> field, select the applicable Threat Prevention Policy for this VSX Gateway object.</li> <li>c. Click <b>Install</b>.</li> </ol>
20	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 1417 711 1446">vsx stat -v</pre>

### 3. Configure the Virtual Devices and their Security Policies in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or each <i>Target</i> Domain Management Server that should manage each Virtual Device.
2	Configure the applicable Virtual Devices on this VSX Gateway.
3	Configure the applicable Access Control Policies for these Virtual Devices.
4	Install the configured Access Control Policies on these Virtual Devices.

Step	Instructions
5	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 384 711 413">vsx stat -v</pre>
6	Configure the applicable Threat Prevention Policies for these Virtual Devices.
7	Install the configured Threat Prevention Policies on these Virtual Devices.
8	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 743 711 772">vsx stat -v</pre>

For more information, see the:

- [R80.40 Security Management Administration Guide](#)
- [R80.40 VSX Administration Guide](#)
- [R80.40 Threat Prevention Administration Guide](#)
- Applicable *Administration Guides* on the [R80.40 Home Page](#).

# Installing a ClusterXL, VSX Cluster, VRRP Cluster

This section provides instructions to install a cluster:

- [\*"Installing a ClusterXL Cluster" on page 105\*](#)
- [\*"Installing a VSX Cluster" on page 123\*](#)
- [\*"Installing a VRRP Cluster" on page 129\*](#)
- [\*"Full High Availability Cluster on Check Point Appliances" on page 143\*](#)

# Installing a ClusterXL Cluster

## Notes:



- This procedure applies to both Check Point Appliances and Open Servers.
- This procedure does **not** apply to Check Point Small Office Appliance models lower than 3000.
- You must install and configure at least two Cluster Members.

## Procedure:

### 1. Install the Cluster Members

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, select these two options:                   <ul style="list-style-type: none"> <li>• <b>Unit is a part of a cluster</b></li> <li>• <b>ClusterXL</b></li> </ul> </li> </ol> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791</a> .

### 2. Configure the ClusterXL object in SmartConsole

You can configure the ClusterXL object in either Wizard Mode, or Classic Mode.

- **Configuring the ClusterXL object in Wizard Mode**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this ClusterXL.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new Cluster object in one of these ways: <ul style="list-style-type: none"> <li>• From the top toolbar, click the <b>New (*) &gt; Cluster &gt; Cluster</b>.</li> <li>• In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; New Cluster</b>.</li> <li>• In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; Cluster</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Cluster Creation</b> window, click <b>Wizard Mode</b> .
5	On the <b>Cluster General Properties</b> page: <ol style="list-style-type: none"> <li>a. In the <b>Cluster Name</b> field, enter the applicable name for this ClusterXL object.</li> <li>b. Configure the main Virtual IP address(es) for this ClusterXL object:               <ul style="list-style-type: none"> <li>• In the <b>Cluster IPv4 Address</b> section, enter the main Virtual IPv4 address for this ClusterXL object.</li> <li>• In the <b>Cluster IPv6 Address</b> section, enter the main Virtual IPv6 address for this ClusterXL object.</li> </ul> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> </li> <li>c. In the <b>Choose the Cluster's Solution</b> field, select <b>Check Point ClusterXL</b> and select the cluster mode - either <b>High Availability</b>, or <b>Load Sharing</b>.</li> <li>d. Click <b>Next</b>.</li> </ol>

Step	Instructions
6	<p>On the <b>Cluster members' properties</b> page, add the objects for the Cluster Members.</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. In the <b>Activation Key</b> and <b>Confirm Activation Key</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>e. Click <b>Initialize</b>.</li> <li>f. Click <b>OK</b>.</li> <li>g. Repeat Steps <b>a-f</b> to add the second Cluster Member, and so on.</li> </ol>

If the **Trust State** field does not show **Trust established**, perform these steps:

- a. Connect to the command line on the Cluster Member.
- b. Make sure there is a physical connectivity between the Cluster Member 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
7	<p>On the <b>Cluster Topology</b> page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>IPv4 Network Address</b> at the top of the page.</li> <li>b. Select the applicable role: <ul style="list-style-type: none"> <li>• For <i>cluster traffic interfaces</i>, select <b>Representing a cluster interface</b> and configure the Cluster Virtual IPv4 address and its Net Mask.</li> </ul>  <p><b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ul style="list-style-type: none"> <li>• For <i>cluster synchronization interfaces</i>, select <b>Cluster Synchronization</b> and select <b>Primary</b> only. Check Point cluster supports only one synchronization network.</li> <li>• For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private use of each member (don't monitor members interfaces)</b>.</li> </ul> </li> <li>c. Click <b>Next</b></li> </ol>
8	<p>On the <b>Cluster Definition Wizard Complete</b> page:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>Configuration Summary</b>.</li> <li>b. Select <b>Edit Cluster's Properties</b>.</li> <li>c. Click <b>Finish</b></li> </ol> <p>The <b>Gateway Cluster Properties</b> window opens.</p>
9	<p>On the <b>General Properties</b> page &gt; <b>Machine</b> section:</p> <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, make sure you see the configured applicable name for this ClusterXL object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard.</li> </ol> <p>Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p>
10	<p>On the <b>General Properties</b> page &gt; <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>

Step	Instructions
11	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL Software Blade</b> is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ol>
12	<p>On the <b>Cluster Members</b> page:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. Click <b>Communication</b>.</li> <li>e. In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>f. Click <b>Initialize</b>.</li> <li>g. Click <b>Close</b>.</li> <li>h. Click <b>OK</b>.</li> <li>i. Repeat Steps <b>a-h</b> to add the second Cluster Member, and so on.</li> </ol> <p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the Cluster Member.</li> <li>b. Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).</li> <li>c. Run: <code>cpconfig</code></li> <li>d. Enter the number of this option: <code>Secure Internal Communication</code></li> <li>e. Follow the instructions on the screen to change the Activation Key.</li> <li>f. In SmartConsole, click <b>Reset</b>.</li> <li>g. Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>h. In SmartConsole, click <b>Initialize</b>.</li> </ol>

Step	Instructions
13	<p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"><li>In the <b>Select the cluster mode and configuration</b> section, select the applicable mode:<ul style="list-style-type: none"><li>• <b>High Availability</b> and <b>ClusterXL</b></li><li>• <b>Load Sharing</b> and <b>Multicast</b> or <b>Unicast</b></li><li>• <b>Active-Active</b> (see the <a href="#"><i>R80.40 ClusterXL Administration Guide</i></a>)</li></ul></li><li>In the <b>Tracking</b> section, select the applicable option.</li><li>In the <b>Advanced Settings</b> section:</li></ol>

Step	Instructions
	<ul style="list-style-type: none"> <li>• If you selected the <b>High Availability</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use State Synchronization</b>. This configures the Cluster Members to synchronize the information about the connections they inspect.</li> </ul> </li> </ul> <p> <b>Best Practice</b> - Enable this setting to prevent connection drops after a cluster failover.</p> <ul style="list-style-type: none"> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> <p><b>Notes:</b></p> <p></p> <ul style="list-style-type: none"> <li>○ This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>○ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>○ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual</b> MAC address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the Cluster Member recovery method - which Cluster Member to select as <b>Active</b> during a fallback (return to normal operation after a cluster failover):             <ul style="list-style-type: none"> <li>○ <b>Maintain current active Cluster Member</b> <ul style="list-style-type: none"> <li>i. The Cluster Member that is currently in the <b>Active</b> state, remains in this state.</li> <li>ii. Other Cluster Members that return to normal operation, remain the <b>Standby</b> state.</li> </ul> </li> <li>○ <b>Switch to higher priority Cluster Member</b> <ul style="list-style-type: none"> <li>i. The Cluster Member that has the highest priority (appears at the top of the list on the <b>Cluster Members</b> page of the cluster object) becomes the new <b>Active</b>.</li> <li>ii. The state of the previously <b>Active</b> Cluster Member changes to <b>Standby</b>.</li> </ul> </li> </ul> </li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>• If you selected the <b>Load Sharing &gt; Multicast</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of all connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>◦ This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. Select the connection sharing method between the Cluster Members:             <ul style="list-style-type: none"> <li>◦ <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members. This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> <li>◦ <b>IPs, Ports</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address and the same Source and Destination ports, regardless of the IPsec SPI numbers. Use this method only if there are problems when the following IP addresses are used: 0.0.0.0, 255.255.255.255, and 127.0.0.1.</li> </ul> </li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>• If you selected the <b>Load Sharing &gt; Unicast</b> mode, then:           <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of all connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>○ This setting in the cluster object applies to all connections that pass through the cluster.</li> <li>○ You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>○ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>○ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual</b> MAC address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the connection sharing method between the Cluster Members:       <ul style="list-style-type: none"> <li>○ <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</li> <li>○ <b>IPs, Ports</b> This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> </ul> </li> </ul>

Step	Instructions
14	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>a. Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li>b. From the left tree, click the <b>General</b> page.</li> <li>c. In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type: <ul style="list-style-type: none"> <li>• For <i>cluster traffic interfaces</i>, select <b>Cluster</b>. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li>• For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>◦ We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li>◦ Check Point cluster supports only one synchronization network.</li> <li>◦ For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li>• For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li>d. In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <ol style="list-style-type: none"> <li>e. In the <b>Topology</b> section: <ul style="list-style-type: none"> <li>• Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li>• Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> </li> </ol>
15	Click <b>OK</b> .
16	Publish the SmartConsole session.

- **Configuring the ClusterXL object in Classic Mode**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this ClusterXL.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new Cluster object in one of these ways: <ul style="list-style-type: none"> <li>• From the top toolbar, click the <b>New (*) &gt; Cluster &gt; Cluster</b>.</li> <li>• In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; New Cluster</b>.</li> <li>• In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; Cluster</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b> . The <b>Gateway Cluster Properties</b> window opens.
5	On the <b>General Properties</b> page > <b>Machine</b> section: <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, make sure you see the configured applicable name for this ClusterXL object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol>
6	On the <b>General Properties</b> page > <b>Platform</b> section, select the correct options: <ol style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
7	On the <b>General Properties</b> page: <ol style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL</b> Software Blade is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ol>

Step	Instructions
8	<p>On the <b>Cluster Members</b> page:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p><b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. Click <b>Communication</b>.</li> <li>e. In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>f. Click <b>Initialize</b>.</li> <li>g. Click <b>Close</b>.</li> <li>h. Click <b>OK</b>.</li> <li>i. Repeat Steps <b>a-h</b> to add the second Cluster Member, and so on.</li> </ol>

If the **Trust State** field does not show **Trust established**, perform these steps:

- a. Connect to the command line on the Cluster Member.
- b. Make sure there is a physical connectivity between the Cluster Member 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
9	<p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"><li>In the <b>Select the cluster mode and configuration</b> section, select the applicable mode:<ul style="list-style-type: none"><li>• <b>High Availability</b> and <b>ClusterXL</b></li><li>• <b>Load Sharing</b> and <b>Multicast or Unicast</b></li><li>• <b>Active-Active</b> (see the <a href="#"><i>R80.40 ClusterXL Administration Guide</i></a>)</li></ul></li><li>In the <b>Tracking</b> section, select the applicable option.</li><li>In the <b>Advanced Settings</b> section:</li></ol>

Step	Instructions
	<ul style="list-style-type: none"> <li>• If you selected the <b>High Availability</b> mode, then:             <ol style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use State Synchronization</b>. This configures the Cluster Members to synchronize the information about the connections they inspect.</li> </ol> </li> </ul> <p> <b>Best Practice</b> - Enable this setting to prevent connection drops after a cluster failover.</p> <ol style="list-style-type: none"> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ol> <p><b>Notes:</b></p> <p></p> <ul style="list-style-type: none"> <li>○ This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>○ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>○ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ol style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual</b> MAC address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the Cluster Member recovery method - which Cluster Member to select as <b>Active</b> during a fallback (return to normal operation after a cluster failover):             <ul style="list-style-type: none"> <li>○ <b>Maintain current active Cluster Member</b> <ol style="list-style-type: none"> <li>i. The Cluster Member that is currently in the <b>Active</b> state, remains in this state.</li> <li>ii. Other Cluster Members that return to normal operation, remain the <b>Standby</b> state.</li> </ol> </li> <li>○ <b>Switch to higher priority Cluster Member</b> <ol style="list-style-type: none"> <li>i. The Cluster Member that has the highest priority (appears at the top of the list on the <b>Cluster Members</b> page of the cluster object) becomes the new <b>Active</b>.</li> <li>ii. The state of the previously <b>Active</b> Cluster Member changes to <b>Standby</b>.</li> </ol> </li> </ul> </li> </ol>

Step	Instructions
	<ul style="list-style-type: none"> <li>• If you selected the <b>Load Sharing &gt; Multicast</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of all connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>◦ This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. Select the connection sharing method between the Cluster Members:             <ul style="list-style-type: none"> <li>◦ <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members. This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> <li>◦ <b>IPs, Ports</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address and the same Source and Destination ports, regardless of the IPsec SPI numbers. Use this method only if there are problems when the following IP addresses are used: 0.0.0.0, 255.255.255.255, and 127.0.0.1.</li> </ul> </li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>• If you selected the <b>Load Sharing &gt; Unicast</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of all connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>○ This setting in the cluster object applies to all connections that pass through the cluster.</li> <li>○ You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>○ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>○ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual</b> MAC address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the connection sharing method between the Cluster Members:             <ul style="list-style-type: none"> <li>○ <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</li> <li>○ <b>IPs, Ports</b> This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> </ul> </li> </ul>

Step	Instructions
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>a. Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li>b. From the left tree, click the <b>General</b> page.</li> <li>c. In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type: <ul style="list-style-type: none"> <li>• For <i>cluster traffic interfaces</i>, select <b>Cluster</b>. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li>• For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>◦ We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li>◦ Check Point cluster supports only one synchronization network.</li> <li>◦ For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li>• For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li>d. In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <ol style="list-style-type: none"> <li>e. In the <b>Topology</b> section: <ul style="list-style-type: none"> <li>• Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li>• Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> </li> </ol>
11	Click <b>OK</b> .
12	Publish the SmartConsole session.

### 3. Configure the applicable Access Control policy for the ClusterXL in SmartConsole

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

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

#### 4. Examine the cluster configuration

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">show cluster state</div> <li>■ In the Expert mode, run:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">cphaprof state</div> </ul>
3	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">show cluster members interfaces all</div> <li>■ In the Expansion Line Card, run:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">cphaprof -a if</div> </ul>

For more information, see the:

- [R80.40 Security Management Administration Guide](#).
- [R80.40 ClusterXL Administration Guide](#).
- Applicable Administration Guides on the [R80.40 Home Page](#).

# Installing a VSX Cluster

## Notes:



- This procedure applies to both Check Point Appliances and Open Servers.
- This procedure does **not** apply to Check Point Small Office Appliance models lower than 3000.
- You must install and configure at least two VSX Cluster Members.

## Procedure:

### 1. Install the VSX Cluster Members

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, select these two options:                   <ul style="list-style-type: none"> <li>• Unit is a part of a cluster</li> <li>• ClusterXL</li> </ul> </li> </ol> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791</a> .

### 2. Configure the VSX Cluster object in SmartConsole



## Notes:

- The steps below are only for a Clean Install of a new VSX Cluster. To configure a VSX Cluster Member that failed, see the [R80.40 VSX Administration Guide](#) > Chapter *Command Line Reference* > Section *vsx\_util* > Section *vsx\_util reconfigure*.
- The steps below are for the Dedicated Management Interfaces (DMI) configuration. For the non-DMI configuration, see the [R80.40 VSX Administration Guide](#).

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Main Domain Management Server</i> that should manage this VSX Cluster.

Step	Instructions
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new VSX Cluster object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (*)</b> &gt; <b>VSX</b> &gt; <b>Cluster</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>VSX</b> &gt; <b>New Cluster</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>VSX</b> &gt; <b>Cluster</b>.</li> </ul>
4	<p>On the <b>VSX Cluster General Properties (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>a. In the <b>Enter the VSX Cluster Name</b> field, enter the applicable name for this VSX Cluster object.</li> <li>b. In the <b>Enter the VSX Cluster IPv4</b> field, enter the Cluster Virtual IPv4 address that is configured on the Dedicated Management Interfaces (DMI).</li> <li>c. In the <b>Enter the VSX Cluster IPv6</b> field, enter the Cluster Virtual IPv6 address that is configured on the Dedicated Management Interfaces (DMI).</li> <li>d. In the <b>Select the VSX Cluster Version</b> field, select <b>R80.40</b>.</li> <li>e. In the <b>Select the VSX Cluster Platform</b> field, select the applicable VSX Cluster mode: <ul style="list-style-type: none"> <li>■ <b>ClusterXL</b> (for High Availability)</li> <li>■ <b>ClusterXL Virtual System Load Sharing</b></li> </ul> </li> <li>f. Click <b>Next</b>.</li> </ol>
5	<p>On the <b>VSX Cluster Members (Define the members of this VSX Cluster)</b> page, add the objects for the VSX Cluster Members:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add</b>.</li> <li>b. In the <b>Cluster Member Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>c. In the <b>Cluster Member IPv4 Address</b> field, enter the IPv4 address of the Dedicated Management Interface (DMI).</li> <li>d. In the <b>Enter the VSX Gateway IPv6</b> field, enter the applicable IPv6 address.</li> <li>e. In the <b>Activation Key</b> and <b>Confirm Activation Key</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>f. Click <b>Initialize</b>.</li> <li>g. Click <b>OK</b>.</li> <li>h. Repeat Steps <b>a-f</b> to add the second VSX Cluster Member, and so on.</li> </ol>

Step	Instructions
	<p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the VSX Cluster Member.</li> <li>Make sure there is a physical connectivity between the VSX Cluster Member and the Management Server (for example, pings can pass).</li> <li>Run:  <pre>cpcconfig</pre> </li> <li>Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpcconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
6	<p>On the <b>VSX Cluster Interfaces (Physical Interfaces Usage)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway.</li> <li>If you plan to connect more than one Virtual System directly to the same physical interface, you must select <b>VLAN Trunk</b> for that physical interface.</li> <li>Click <b>Next</b>.</li> </ol>
7	<p>On the <b>VSX Cluster members (Synchronization Network)</b> page:</p> <ol style="list-style-type: none"> <li>Select the interface that will be used for state synchronization.</li> <li>Configure the IPv4 addresses for the Sync interfaces on each Cluster Member.</li> <li>Click <b>Next</b>.</li> </ol>
8	<p>On the <b>Virtual Network Device Configuration (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>You can select <b>Create a Virtual Network Device</b> and configure the first applicable Virtual Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router.</li> <li>Click <b>Next</b>.</li> </ol>
9	<p>On the <b>VSX Gateway Management (Specify the management access rules)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the default access rules.</li> <li>Select the applicable default access rules.</li> <li>Configure the applicable source objects, if needed.</li> <li>Click <b>Next</b>.</li> </ol> <p> <b>Important</b> - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.</p>
10	<p>On the <b>VSX Gateway Creation Finalization</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Finish</b> and wait for the operation to finish.</li> <li>Click <b>View Report</b> for more information.</li> <li>Click <b>Close</b>.</li> </ol>

Step	Instructions
11	<p>Examine the VSX Cluster configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on each VSX Cluster Member.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 384 711 413">&gt; vsx stat -v</pre>
12	<p>In SmartConsole, open the VSX Cluster object.</p>
13	<p>On the <b>General Properties</b> page &gt; the <b>Network Security</b> tab:</p> <ol style="list-style-type: none"> <li>a. Make sure the <b>ClusterXL</b> Software Blade is selected.</li> <li>b. Enable the additional applicable Software Blades for the VSX Cluster object itself (context of VS0).</li> </ol> <p>Refer to:</p> <ul style="list-style-type: none"> <li>■ <a href="#">sk79700: VSX supported features on R75.40VS and above</a></li> <li>■ <a href="#">sk106496: Software Blades updates on VSX R75.40VS and above - FAQ</a></li> <li>■ Applicable <i>Administration Guides</i> on the <a href="#">R80.40 Home Page</a>.</li> </ul>
14	<p>Click <b>OK</b> to push the updated VSX Configuration.      Click <b>View Report</b> for more information.</p>
15	<p>Install the default policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> <li>a. Click <b>Install Policy</b>.</li> <li>b. In the <b>Policy</b> field, select the default policy for this VSX Cluster object.          This policy is called:  <code data-bbox="520 1102 1060 1131">&lt;Name of VSX Cluster object&gt;_VSX</code> </li> <li>c. Click <b>Install</b>.</li> </ol>

Step	Instructions
16	<p>Examine the VSX configuration and cluster state:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on <i>each</i> VSX Cluster Member.</li> <li>b. Examine the VSX configuration: In the Expert mode, run:</li> </ol> <pre data-bbox="520 384 711 411">vsx stat -v</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul> <ol style="list-style-type: none"> <li>c. Examine the cluster state in one of these ways:       <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre data-bbox="600 669 949 727">set virtual-system 0 show cluster state</pre> </li> <li>■ In the Expert mode, run:           <pre data-bbox="600 804 843 862">vsenv 0 cphaprof state</pre> </li> </ul> </li> </ol> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members.</li> <li>■ One VSX Cluster Member must be in the <b>Active</b> state, and all other VSX Cluster Members must be in <b>Standby</b> state.</li> <li>■ All Virtual Systems must show the same information about the states of all Virtual Systems.</li> </ul> <ol style="list-style-type: none"> <li>d. Examine the cluster interfaces in one of these ways:       <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre data-bbox="600 1230 1192 1289">set virtual-system 0 show cluster members interfaces all</pre> </li> <li>■ In the Expert mode, run:           <pre data-bbox="600 1365 843 1423">vsenv 0 cphaprof -a if</pre> </li> </ul> </li> </ol>

### 3. Configure the Virtual Devices and their Security Policies in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or each <i>Target</i> Domain Management Server that should manage each Virtual Device.
2	Configure the applicable Virtual Devices on this VSX Cluster.
3	Configure the applicable Access Control and Threat Prevention Policies for these Virtual Devices.
4	Install the configured Security Policies on these Virtual Devices.

Step	Instructions
5	<p>Examine the VSX configuration and cluster state:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on <i>each</i> VSX Cluster Member.</li> <li>b. Examine the VSX configuration: In the Expert mode, run:</li> </ol> <pre data-bbox="520 384 711 411">vsx stat -v</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul> <ol style="list-style-type: none"> <li>c. Examine the cluster state in one of these ways:       <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre data-bbox="600 669 949 736">set virtual-system 0 show cluster state</pre> </li> <li>■ In the Expert mode, run:           <pre data-bbox="600 804 854 871">vsenv 0 cphaprof state</pre> </li> </ul> </li> </ol> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members.</li> <li>■ One VSX Cluster Member must be in the <b>Active</b> state, and all other VSX Cluster Members must be in <b>Standby</b> state.</li> <li>■ All Virtual Systems must show the same information about the states of all Virtual Systems.</li> </ul> <ol style="list-style-type: none"> <li>d. Examine the cluster interfaces in one of these ways:       <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre data-bbox="600 1230 1203 1298">set virtual-system 0 show cluster members interfaces all</pre> </li> <li>■ In the Expert mode, run:           <pre data-bbox="600 1365 854 1432">vsenv 0 cphaprof -a if</pre> </li> </ul> </li> </ol>

For more information, see the:

- [R80.40 Security Management Administration Guide](#).
- [R80.40 VSX Administration Guide](#).
- [R80.40 ClusterXL Administration Guide](#).
- Applicable *Administration Guides* on the [R80.40 Home Page](#).

# Installing a VRRP Cluster

**Notes:**



- This procedure applies to both Check Point Appliances and Open Servers.
- This procedure does **not** apply to Check Point Small Office Appliance models lower than 3000.
- VRRP Cluster on Gaia supports only two Cluster Members (see [sk105170](#)).

**Procedure:**

1. **Install the VRRP Cluster Members**

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, select these two options:                   <ul style="list-style-type: none"> <li>• Unit is a part of a cluster</li> <li>• VRRP Cluster</li> </ul> </li> </ol> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	Install a valid license. See <a href="#">"Working with Licenses" on page 791</a> .
5	On Gaia, VRRP can be used with ClusterXL <i>enabled</i> or with ClusterXL <i>disabled</i> . See the <a href="#">R80.40 Gaia Administration Guide</a> - Chapter <i>High Availability</i> for more information. If it is necessary to configure VRRP with ClusterXL <i>enabled</i> , then: <ol style="list-style-type: none"> <li>a. When prompted to reboot, click <b>Cancel</b>.</li> <li>b. Connect to the command line.</li> <li>c. Run:               <pre>cpconfig</pre>             d. Select <b>Enable cluster membership for this gateway</b> to enable State synchronization.                Enter <b>y</b> when prompted.             </li> <li>e. Exist from the cpconfig menu.</li> </ol>
6	Reboot.

2. **Perform the initial VRRP configuration in Gaia on the VRRP Cluster Members**

Configure the VRRP in Gaia on both Cluster Members.

Follow the instructions in the [R80.40 Gaia Administration Guide](#) - Chapter *High Availability*.

In addition, refer to:

- [sk105170: Configuration requirements / considerations and limitations for VRRP cluster on Gaia OS](#)
- [sk92061: How to configure VRRP on Gaia](#)

### 3. Configure the VRRP Cluster object in SmartConsole

## ■ Configuring in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this VRRP Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new Cluster object in one of these ways: <ul style="list-style-type: none"> <li>• From the top toolbar, click the <b>New (*) &gt; Cluster &gt; Cluster</b>.</li> <li>• In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; New Cluster</b>.</li> <li>• In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; Cluster</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Cluster Creation</b> window, click <b>Wizard Mode</b> .
5	On the <b>Cluster General Properties</b> page: <ol style="list-style-type: none"> <li>a. In the <b>Cluster Name</b> field, enter the applicable name for this VRRP Cluster object.</li> <li>b. Configure the main Virtual IP address(es) for this VRRP Cluster object.               <ul style="list-style-type: none"> <li>• In the <b>Cluster IPv4 Address</b> section, enter the main Virtual IPv4 address for this VRRP Cluster object.</li> <li>• In the <b>Cluster IPv6 Address</b> section, enter the main Virtual IPv6 address for this VRRP Cluster object.</li> </ul>  <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.             </li> <li>c. In the <b>Choose the Cluster's Solution</b> field, select <b>Gaia VRRP</b>.</li> <li>d. Click <b>Next</b>.</li> </ol>

Step	Instructions
6	<p>On the <b>Cluster members' properties</b> page, add the objects for the Cluster Members.</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this VRRP Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. In the <b>Activation Key</b> and <b>Confirm Activation Key</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>e. Click <b>Initialize</b>.</li> <li>f. Click <b>OK</b>.</li> <li>g. Repeat Steps <b>a-f</b> to add the second VRRP Cluster Member.</li> </ol>

If the **Trust State** field does not show **Trust established**, perform these steps:

- a. Connect to the command line on the Cluster Member.
- b. Make sure there is a physical connectivity between the Cluster Member 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
7	<p>On the <b>Cluster Topology</b> page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>IPv4 Network Address</b> at the top of the page.</li> <li>b. Select the applicable role: <ul style="list-style-type: none"> <li>• For <i>cluster traffic interfaces</i>, select <b>Representing a cluster interface</b> and configure the Cluster Virtual IPv4 address and its Net Mask.</li> </ul> </li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ul style="list-style-type: none"> <li>• For <i>cluster synchronization interfaces</i>, select <b>Cluster Synchronization</b> and select <b>Primary</b> only. Check Point cluster supports only one synchronization network.</li> <li>• For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private use of each member (don't monitor members interfaces)</b>.</li> </ul> <p>c. Click <b>Next</b></p>
8	<p>On the <b>Cluster Definition Wizard Complete</b> page:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>Configuration Summary</b>.</li> <li>b. Select <b>Edit Cluster's Properties</b>.</li> <li>c. Click <b>Finish</b></li> </ol> <p>The <b>Gateway Cluster Properties</b> window opens.</p>
9	<p>On the <b>General Properties</b> page &gt; <b>Machine</b> section:</p> <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, enter the applicable name for this VRRP Cluster object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard.</li> </ol> <p>Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p>
10	<p>On the <b>General Properties</b> page &gt; <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>

Step	Instructions
11	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL Software Blade</b> is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ol>
12	<p>On the <b>Cluster Members</b> page:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this VRRP Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this VRRP Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. Click <b>Communication</b>.</li> <li>e. In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>f. Click <b>Initialize</b>.</li> <li>g. Click <b>Close</b>.</li> <li>h. Click <b>OK</b>.</li> <li>i. Repeat Steps <b>a-h</b> to add the second Cluster Member.</li> </ol> <p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the Cluster Member.</li> <li>b. Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).</li> <li>c. Run: <code>cpconfig</code></li> <li>d. Enter the number of this option: <code>Secure Internal Communication</code></li> <li>e. Follow the instructions on the screen to change the Activation Key.</li> <li>f. In SmartConsole, click <b>Reset</b>.</li> <li>g. Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>h. In SmartConsole, click <b>Initialize</b>.</li> </ol>

Step	Instructions
13	<p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"><li>a. In the <b>Select the cluster mode and configuration</b> section, select <b>High Availability and VRRP</b>.</li><li>b. In the <b>Tracking</b> section, select the applicable option.</li><li>c. In the <b>Advanced Settings</b> section:<ul style="list-style-type: none"><li>• Optional: Select <b>Use State Synchronization</b></li><li>• Optional: Select <b>Hide Cluster Members outgoing traffic behind the Cluster IP Address</b></li><li>• Optional: Select <b>Forward Cluster incoming traffic to Cluster Members IP Addresses</b></li></ul></li></ol> <p>For more information, click the (?) button in the top right corner.</p> <p> <b>Best Practice</b> - We recommend to select all these optional settings.</p>

Step	Instructions
14	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>a. Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li>b. From the left tree, click the <b>General</b> page.</li> <li>c. In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type: <ul style="list-style-type: none"> <li>• For <i>cluster traffic interfaces</i>, select <b>Cluster</b>. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li>• For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>◦ We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li>◦ Check Point cluster supports only one synchronization network.</li> <li>◦ For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li>• For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li>d. In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <ol style="list-style-type: none"> <li>e. In the <b>Topology</b> section: <ul style="list-style-type: none"> <li>• Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li>• Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> </li> </ol>
15	Click <b>OK</b> .
16	Publish the SmartConsole session.

## ■ Configuring in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this VRRP Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> <li>• From the top toolbar, click the <b>New (*) &gt; Cluster &gt; Cluster</b>.</li> <li>• In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; New Cluster</b>.</li> <li>• In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; Cluster</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Cluster Creation</b> window, click <b>Classic Mode</b>. The <b>Gateway Cluster Properties</b> window opens.</p>
5	<p>On the <b>General Properties</b> page &gt; <b>Machine</b> section:</p> <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, enter the applicable name for this VRRP Cluster object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol>
6	<p>On the <b>General Properties</b> page &gt; <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
7	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL Software Blade</b> is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ol>

Step	Instructions
8	<p>On the <b>Cluster Members</b> page:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this VRRP Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this VRRP Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p><b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. Click <b>Communication</b>.</li> <li>e. In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>f. Click <b>Initialize</b>.</li> <li>g. Click <b>Close</b>.</li> <li>h. Click <b>OK</b>.</li> <li>i. Repeat Steps <b>a-h</b> to add the second Cluster Member.</li> </ol>

If the **Trust State** field does not show **Trust established**, perform these steps:

- a. Connect to the command line on the Cluster Member.
- b. Make sure there is a physical connectivity between the Cluster Member 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
9	<p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"><li>a. In the <b>Select the cluster mode and configuration</b> section, select <b>High Availability</b> and <b>VRRP</b>.</li><li>b. In the <b>Tracking</b> section, select the applicable option.</li><li>c. In the <b>Advanced Settings</b> section:<ul style="list-style-type: none"><li>• Optional: Select <b>Use State Synchronization</b></li><li>• Optional: Select <b>Hide Cluster Members outgoing traffic behind the Cluster IP Address</b></li><li>• Optional: Select <b>Forward Cluster incoming traffic to Cluster Members IP Addresses</b></li></ul></li></ol> <p>For more information, click the (?) button in the top right corner.</p> <p> <b>Best Practice</b> - We recommend to select all these optional settings.</p>

Step	Instructions
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li data-bbox="568 265 1356 332">a. Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li data-bbox="568 332 1117 366">b. From the left tree, click the <b>General</b> page.</li> <li data-bbox="568 366 1340 433">c. In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type:           <ul style="list-style-type: none"> <li data-bbox="657 444 1219 478">• For <i>cluster traffic interfaces</i>, select <b>Cluster</b>.</li> <li data-bbox="689 478 1435 545">Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li data-bbox="657 545 1340 613">• For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li data-bbox="854 653 1387 720">◦ We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li data-bbox="854 720 1356 788">◦ Check Point cluster supports only one synchronization network.</li> <li data-bbox="854 788 1467 923">◦ For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li data-bbox="657 934 1340 1001">• For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li data-bbox="568 1006 1276 1073">d. In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <ol style="list-style-type: none"> <li data-bbox="568 1282 911 1316">e. In the <b>Topology</b> section:           <ul style="list-style-type: none"> <li data-bbox="657 1320 1356 1388">• Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li data-bbox="657 1388 1171 1421">• Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> </li> </ol>
11	Click <b>OK</b> .
12	Publish the SmartConsole session.

#### 4. Configure the Security Policy for the VRRP Cluster in SmartConsole

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

Step	Instructions																		
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> <li>a. At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>b. On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>c. In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>d. Click <b>Close</b>.</li> <li>e. On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>																		
4	<p>Create the required Access Control rules.</p> <p>You must define an explicit Access Control rule to allow the VRRP Cluster Members to send and receive the VRRP and IGMP traffic:</p> <table border="1" data-bbox="377 646 1457 945"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>VRRP and IGMP</td> <td>VRRP Cluster object</td> <td>Node Host object with IP address 224.0.0.18</td> <td>Any</td> <td>vrrp igmp</td> <td>Accept</td> <td>None</td> <td>VRRP Cluster object</td> </tr> </tbody> </table>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install	1	VRRP and IGMP	VRRP Cluster object	Node Host object with IP address 224.0.0.18	Any	vrrp igmp	Accept	None	VRRP Cluster object
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install											
1	VRRP and IGMP	VRRP Cluster object	Node Host object with IP address 224.0.0.18	Any	vrrp igmp	Accept	None	VRRP Cluster object											
	<p>If the VRRP Cluster Members use dynamic routing protocols (such as OSPF or RIP), create new rules for each multicast destination IP address.</p> <p>Alternatively, you can create a <b>Network</b> object to represent all multicast network IP destinations:</p> <ul style="list-style-type: none"> <li>■ Name: MCAST.NET (this is an example name)</li> <li>■ IP Address: 224.0.0.0</li> <li>■ Net mask: 240.0.0.0</li> </ul> <p>You can use one rule for all multicast protocols you agree to accept, as shown in this example:</p> <table border="1" data-bbox="377 1304 1457 1603"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>All multicast protocols</td> <td>VRRP Cluster object</td> <td>VRRP Cluster object MCAST.NET</td> <td>Any</td> <td>vrrp igmp ospf rip</td> <td>Accept</td> <td>None</td> <td>VRRP Cluster object</td> </tr> </tbody> </table>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install	1	All multicast protocols	VRRP Cluster object	VRRP Cluster object MCAST.NET	Any	vrrp igmp ospf rip	Accept	None	VRRP Cluster object
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install											
1	All multicast protocols	VRRP Cluster object	VRRP Cluster object MCAST.NET	Any	vrrp igmp ospf rip	Accept	None	VRRP Cluster object											
5	Configure additional applicable Access Control rules.																		
6	Install the Access Control Policy on the VRRP Cluster object.																		
7	Configure and install the applicable Threat Prevention Policy on the VRRP Cluster object.																		

## 5. Examine the cluster configuration

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: show cluster state</li> <li>■ In the Expert mode, run: cphaprof state</li> </ul>
3	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: show cluster members interfaces all</li> <li>■ In the Expert mode, run: cphaprof -a if</li> </ul>
4	<p>Examine the VRRP configuration in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: show vrrp</li> <li>■ In the Expert mode, run: clish -c "show vrrp"</li> </ul>

For more information, see the:

- [R80.40 Security Management Administration Guide](#).
- [R80.40 ClusterXL Administration Guide](#).
- [R80.40 Gaia Administration Guide](#).
- Applicable *Administration Guides* on the [R80.40 Home Page](#).
- [sk105170: Configuration requirements / considerations and limitations for VRRP cluster on Gaia OS](#)
- [sk92061: How to configure VRRP on Gaia](#)

# Full High Availability Cluster on Check Point Appliances

This section provides instructions to install a Full High Availability Cluster.

# Understanding Full High Availability Cluster on Appliances

In a Full High Availability Cluster on two Check Point Appliances, each appliance runs both as a ClusterXL Cluster Member and as a Security Management Server, in High Availability mode.



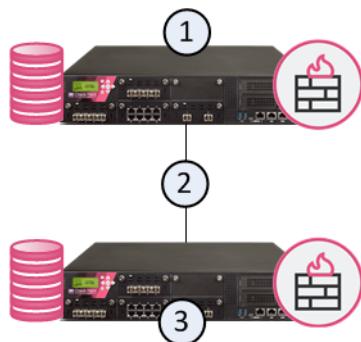
**Important** - You can deploy and configure a Full High Availability Cluster only on Check Point Appliances that support Standalone configuration. See the [R80.40 Release Notes](#) and ["Installing a Standalone" on page 150](#).

This deployment reduces the maintenance required for your systems.

In the image below, the appliances are denoted as (1) and (3).

The two appliances are connected with a direct synchronization connection (2) and work in High Availability mode:

- The Security Management Server on one appliance (for example, 1) runs as Primary, and the Security Management Server on the other appliance (3) runs as Secondary.
- The ClusterXL on one appliance (for example, 1) runs as Active, and the ClusterXL on the other appliance (3), runs as Standby.
- The ClusterXL Cluster Members synchronize the information about the traffic over the synchronization connection (2).



For information on ClusterXL functionality, see the [R80.40 ClusterXL Administration Guide](#).

For information on Security Management Servers, see the [R80.40 Security Management Administration Guide](#).



**Important** - SmartEvent Server is not supported in Management High Availability and Full High Availability Cluster environments ([sk25164](#)). For these environments, install a Dedicated SmartEvent Server (see ["Installing a Dedicated Log Server or SmartEvent Server" on page 67](#)).

# Installing Full High Availability Cluster

## Procedure:

1. Install the first Cluster Member of the Full High Availability Cluster that runs the Primary Security Management Server

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Products</b> section, select both <b>Security Gateway</b> and <b>Security Management</b>.</li> <li>b. In the <b>Clustering</b> section: <ul style="list-style-type: none"> <li>• Select <b>Unit is a part of a cluster, type</b> and select <b>ClusterXL</b>.</li> <li>• In the <b>Define Security Management as</b> field, select <b>Primary</b>.</li> </ul> </li> </ul> </li> <li>■ In the <b>Security Management Administrator</b> window, select one of these options: <ul style="list-style-type: none"> <li>• <b>Use Gaia administrator</b></li> <li>• <b>Define a new administrator</b> and configure it</li> </ul> </li> <li>■ In the <b>Security Management GUI Clients</b> window, configure the applicable allowed computers: <ul style="list-style-type: none"> <li>• <b>Any IP Address</b> - Allows all computers to connect</li> <li>• <b>This machine</b> - Allows only the single specified computer to connect</li> <li>• <b>Network</b> - Allows all computers on the specified network to connect</li> <li>• <b>Range of IPv4 addresses</b> - Allows all computers in the specified range to connect</li> </ul> </li> </ul>
4	<p>Install a valid license.</p> <p>See <a href="#">"Working with Licenses" on page 791</a>.</p>
5	<p>With a web browser, connect to Gaia Portal at:</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <a href="https://&lt;IP address of Gaia Management Interface&gt;">https://&lt;IP address of Gaia Management Interface&gt;</a> </div>
6	<p>In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b>. Configure all required interfaces with applicable unique IP addresses.</p>

2. Install the second Cluster Member of the Full High Availability Cluster that runs the

## Secondary Security Management Server

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:             <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select both <b>Security Gateway</b> and <b>Security Management</b>.</li> <li>b. In the <b>Clustering</b> section:                     <ul style="list-style-type: none"> <li>• Select <b>Unit is a part of a cluster, type</b> and select <b>ClusterXL</b>.</li> <li>• In the <b>Define Security Management as</b> field, select <b>Secondary</b>.</li> </ul> </li> </ol> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>
4	<p>Install a valid license.</p> <p>See <a href="#">"Working with Licenses" on page 791</a>.</p>
5	<p>With a web browser, connect to Gaia Portal at:</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <a href="https://&lt;IP address of Gaia Management Interface&gt;">https://&lt;IP address of Gaia Management Interface&gt;</a> </div>
6	<p>In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b>. Configure all required interfaces with applicable unique IP addresses.</p>

### 3. Connect the synchronization interfaces on both appliances

Step	Instructions
1	<p>Connect a cable between the synchronization interfaces on both appliances.</p> <p>See the <a href="#">R80.40 ClusterXL Administration Guide</a> - Chapter <i>ClusterXL Requirements and Compatibility</i> - Section <i>Supported Topologies for Synchronization Network</i>.</p>
2	<p>With a web browser, connect to Gaia Portal on both appliances at:</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <a href="https://&lt;IP address of Gaia Management Interface&gt;">https://&lt;IP address of Gaia Management Interface&gt;</a> </div>
3	In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b> .
4	In the top right corner, click the <b>Configuration</b> button.
5	Make sure the <b>Link Status</b> on the synchronization interfaces is <b>Up</b> .
6	In the top right corner, click the <b>Monitoring</b> button.

Step	Instructions
7	<p>Click <b>Refresh</b> every several seconds. These counters must increase:</p> <ul style="list-style-type: none"> <li>■ <b>Rbytes</b></li> <li>■ <b>Rpackets</b></li> <li>■ <b>Tbytes</b></li> <li>■ <b>Tpackets</b></li> </ul>

#### 4. Install the R80.40 SmartConsole

Follow "["Installing SmartConsole" on page 89.](#)

#### 5. Configure the Full High Availability Cluster object in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Cluster Member that runs the <b>Primary Security Management Server</b> .
2	In the <b>Security Cluster wizard</b> , click <b>Next</b> .
3	Enter the name of the Full High Availability Cluster object.
4	Click <b>Next</b> .
5	Configure the settings for the Full High Availability Cluster Member that runs the <b>Secondary Security Management Server</b> : <ol style="list-style-type: none"> <li>a. In the <b>Secondary Member Name</b> field, enter the hostname that you entered during the First Time Configuration Wizard.</li> <li>b. In the <b>Secondary Member Name IP Address</b> field, enter the IP address of the Gaia Management Interface that you entered during the First Time Configuration Wizard.</li> <li>c. Enter and confirm the SIC <b>Activation Key</b> that you entered during the First Time Configuration Wizard.</li> </ol>
6	Click <b>Next</b> .
7	Configure the IP address of the paired interfaces on the appliances. Select one of these options: <ul style="list-style-type: none"> <li>■ <b>Cluster Interface with Virtual IP</b> - Enter a Cluster Virtual IP address for the interface.</li> <li>■ <b>Cluster Sync Interface</b> - Configure the interface as the synchronization interface for the appliances.</li> <li>■ <b>Non-Cluster Interface</b> - Use the configured IP address of this interface.</li> </ul>
8	Click <b>Next</b> .
9	Repeat Step 7 for all the interfaces.
10	Click <b>Finish</b> .

Step	Instructions
11	Publish the SmartConsole session.
12	Install the Access Control Policy on this cluster object. Only after policy installation, can the Primary server synchronize with the Secondary server.
13	Install the Threat Prevention Policy on this cluster object.



**Note** - You can also control the Full High Availability Cluster Members in Gaia Portal > **High Availability > Cluster** page.

For more information, see the:

- [R80.40 Gaia Administration Guide](#)
- [R80.40 ClusterXL Administration Guide](#)

# Recommended Logging Options for a Full High Availability Cluster

In a cluster, log files are not synchronized between the two Cluster Members.



**Best Practice** - We recommend that you install a dedicated Log Server and configure the Cluster Members to forward their logs to that dedicated Log Server.

Step	Instructions
1	Install a dedicated Log Server. Follow " <a href="#">Installing a Dedicated Log Server or SmartEvent Server</a> " on page 67.
2	Connect with SmartConsole to the Full High Availability Cluster Member that runs the Primary Security Management Server.
3	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
4	Open the cluster object.
5	From the left navigation tree, click <b>Logs &gt; Additional Logging Configuration</b> .
6	Select <b>Forward log files to Log Server</b> and select the object of the dedicated Log Server.
7	In the <b>Log forwarding schedule</b> field, select or define a <b>Scheduled Event</b> object.
8	Click <b>OK</b> .
9	Publish the SmartConsole session.
10	Install the Access Control Policy on this cluster object.

# Installing a Standalone

In a Standalone deployment, a Check Point computer runs both the Security Gateway and Security Management Server products.

**Important:**



- These instructions apply only to Check Point Appliances that support a Standalone deployment.
- These instructions apply to all Open Servers.
- These instructions apply to Virtual Machines.

See the [\*R80.40 Release Notes\*](#) for the requirements for a Standalone deployment.

These methods are available to configure a Standalone deployment:

## Configuring a Standalone in Standard Mode

This method is supported on Check Point appliances (that support a Standalone deployment), Open Servers, and Virtual Machines that meet the requirements listed in the [\*R80.40 Release Notes\*](#).

## 1. Install the Standalone

Step	Instructions
1	<p>Install the Gaia Operating System:</p> <ul style="list-style-type: none"> <li>■ <a href="#"><i>"Installing the Gaia Operating System on Check Point Appliances" on page 31</i></a></li> <li>■ <a href="#"><i>"Installing the Gaia Operating System on Open Servers" on page 33</i></a></li> </ul>
2	Follow <a href="#"><i>"Configuring Gaia for the First Time" on page 38.</i></a>
3	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Products</b> section, select both <b>Security Gateway</b> and <b>Security Management</b>.</li> <li>b. In the <b>Clustering</b> section: <ul style="list-style-type: none"> <li>• Clear <b>Unit is a part of a cluster, type</b>.</li> <li>• In the <b>Define Security Management as</b> field, select <b>Primary</b>.</li> </ul> </li> </ul> </li> <li>■ In the <b>Security Management Administrator</b> window, select one of these options: <ul style="list-style-type: none"> <li>• <b>Use Gaia administrator</b></li> <li>• <b>Define a new administrator</b> and configure it</li> </ul> </li> <li>■ In the <b>Security Management GUI Clients</b> window, configure the applicable allowed computers: <ul style="list-style-type: none"> <li>• <b>Any IP Address</b> - Allows all computers to connect</li> <li>• <b>This machine</b> - Allows only the single specified computer to connect</li> <li>• <b>Network</b> - Allows all computers on the specified network to connect</li> <li>• <b>Range of IPv4 addresses</b> - Allows all computers in the specified range to connect</li> </ul> </li> </ul>

## 2. Configure the Standalone object in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Standalone.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Open the Standalone object.  <b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>

Step	Instructions
4	<p>In the <b>Platform</b> section, select the correct options:</p> <ul style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: <ul style="list-style-type: none"> <li>■ If you install the Security Gateway on a Check Point Appliance, select the correct appliances series.</li> <li>■ If you install the Security Gateway on an Open Server, select <b>Open server</b>.</li> </ul> </li> <li>b. Make sure the <b>Version</b> field shows <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ul>
5	Enable the applicable Software Blades: <ul style="list-style-type: none"> <li>■ On the <b>Network Security</b> tab.</li> <li>■ On the <b>Threat Prevention</b> tab.</li> </ul>
6	On the <b>Management</b> tab, enable the applicable Software Blades.
7	Click <b>OK</b> .
8	Publish the SmartConsole session.

### 3. Configure the applicable Access Control policy for the Standalone in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Standalone.
2	From the left navigation panel, click <b>Security Policies</b> .
3	Create a new policy and configure the applicable layers: <ul style="list-style-type: none"> <li>a. At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>b. On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>c. In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>d. Click <b>Close</b>.</li> <li>e. On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ul>
4	Create the applicable Access Control rules.
5	Install the Access Control Policy on the Standalone object.

## Configuring a Standalone in Quick Setup Mode

This method is supported only on Check Point appliances that support a Standalone deployment.

This method installs a Standalone on a Check Point appliance in **Bridge Mode**.

For more information on Gaia Quick Standalone Setup on Check Point appliances, see [sk102231](#).

For more information, see the:

- [\*R80.40 Security Management Administration Guide\*](#).
- Applicable *Administration Guides* on the [\*R80.40 Home Page\*](#).

# Post-Installation Configuration

After the installation is complete, and you rebooted the Check Point computer:

- Configure the applicable settings in the Check Point Configuration Tool.
- Check the recommended and available software packages in CPUSE (see "[Installing Software Packages on Gaia" on page 160](#)).

**The Check Point Configuration Tool lets you configure these settings:**

Check Point computer	Commands	Available Configuration Options
Security Management Server, Dedicated Log Server, Dedicated SmartEvent Server	cpconfig	<ul style="list-style-type: none"> <li>(1) Licenses and contracts</li> <li>(2) Administrator</li> <li>(3) GUI Clients</li> <li>(4) SNMP Extension</li> <li>(5) Random Pool</li> <li>(6) Certificate Authority</li> <li>(7) Certificate's Fingerprint</li> <li>(8) Automatic start of Check Point Products</li>   <li>(9) Exit</li> </ul>
Multi-Domain Server, Multi-Domain Log Server	1. mdsenv 2. mdsconfig	<ul style="list-style-type: none"> <li>(1) Leading VIP Interfaces</li> <li>(2) Licenses</li> <li>(3) Random Pool</li> <li>(4) Groups</li> <li>(5) Certificate's Fingerprint</li> <li>(6) Administrators</li> <li>(7) GUI clients</li> <li>(8) Automatic Start of Multi-Domain Server</li> <li>(9) P1Shell</li> <li>(10) Start Multi-Domain Server Password</li> <li>(11) IPv6 Support for Multi-Domain Server</li> <li>(12) IPv6 Support for Existing Domain Management Servers</li>   <li>(13) Exit</li> </ul>

Check Point computer	Commands	Available Configuration Options
Security Gateway, Cluster Member	cpconfig	<ul style="list-style-type: none"> <li>(1) Licenses and contracts</li> <li>(2) SNMP Extension</li> <li>(3) PKCS#11 Token</li> <li>(4) Random Pool</li> <li>(5) Secure Internal Communication</li> <li>(6) Disable cluster membership for this gateway</li> <li>(7) Enable Check Point Per Virtual System State</li> <li>(8) Enable Check Point ClusterXL for Bridge Active/Standby</li> <li>(9) Check Point CoreXL</li> <li>(10) Automatic start of Check Point Products</li> <li>(11) Exit</li> </ul>

### Explanation about the Configuration Options on a Security Management Server, dedicated Log Server or SmartEvent Server

For more information, see the [R80.40 Security Management Administration Guide](#).



**Note** - The options shown depend on the configuration and installed products.

Menu Option	Description
Licenses and contracts	Manages Check Point licenses and contracts on this server.
Administrator	Configures Check Point system administrators for this server.
GUI Clients	Configures the GUI clients that can use SmartConsole to connect to this server.
SNMP Extension	Obsolete. Do not use this option anymore. To configure SNMP, see the <a href="#">R80.40 Gaia Administration Guide</a> - Chapter <i>System Management</i> - Section <i>SNMP</i> .
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.
Certificate Authority	Initializes the Internal Certificate Authority (ICA) and configures the Certificate Authority's (CA) Fully Qualified Domain Name (FQDN).
Certificate's Fingerprint	Shows the ICA's Fingerprint. This fingerprint is a text string derived from the server's ICA certificate. This fingerprint verifies the identity of the server when you connect to it with SmartConsole.

Menu Option	Description
<b>Automatic start of Check Point Products</b>	Shows and controls which of the installed Check Point products start automatically during boot.
<b>Exit</b>	Exits from the Check Point Configuration Tool.

### Explanation about the Configuration Options on a Multi-Domain Server or Multi-Domain Log Server

For more information, see the [\*R80.40 Multi-Domain Security Management Administration Guide\*](#).

Menu Option	Description
<b>Leading VIP Interfaces</b>	<p>The Leading VIP Interfaces are real interfaces connected to an external network.</p> <p>These interfaces are used when you configure virtual IP addresses for Domain Management Servers.</p>
<b>Licenses</b>	Manages Check Point licenses and contracts on this server.
<b>Random Pool</b>	Configures the RSA keys, to be used by Gaia Operating System.
<b>Groups</b>	<p>Usually, the Multi-Domain Server is given group permission for access and execution.</p> <p>You may now name such a group or instruct the installation procedure to give no group permissions to the server.</p> <p>In the latter case, only the Super-User is able to access and execute commands on the server.</p>
<b>Certificate's Fingerprint</b>	<p>Shows the ICA's Fingerprint.</p> <p>This fingerprint is a text string derived from the server's ICA certificate.</p> <p>This fingerprint verifies the identity of the server when you connect to it with SmartConsole.</p>
<b>Administrators</b>	Configures Check Point system administrators for this server.
<b>GUI Clients</b>	Configures the GUI clients that can use SmartConsole to connect to this server.
<b>Automatic Start of Multi-Domain Server</b>	Shows and controls if Multi-Domain Server starts automatically during boot.
<b>P1Shell</b>	<p>Obsolete. Do <b>not</b> use this option anymore.</p> <p> <b>Important</b> - This option and the <code>p1shell</code> command are <b>not</b> supported (Known Limitation PMTR-45085).</p>
<b>Start Multi-Domain Server Password</b>	Configures a password to control the start of the Multi-Domain Server.
<b>IPv6 Support for Multi-Domain Server</b>	<p>Enables or disables the IPv6 Support on the Multi-Domain Server.</p> <p> <b>Important</b> - R80.40 Multi-Domain Server does <b>not</b> support IPv6 address configuration (Known Limitation PMTR-14989).</p>

Menu Option	Description
<b>IPv6 Support for Existing Domain Management Servers</b>	Enables or disables the IPv6 Support on the Domain Management Servers.   <b>Important</b> - R80.40 Multi-Domain Server does not support IPv6 address configuration (Known Limitation PMTR-14989).
<b>Exit</b>	Exits from the Multi-Domain Server Configuration Program.

### Explanation about the Configuration Options on a Security Gateway or Cluster Member



**Note** - The options shown depend on the configuration and installed products.

Menu Option	Description
<b>Licenses and contracts</b>	Manages Check Point licenses and contracts on this Security Gateway or Cluster Member.
<b>SNMP Extension</b>	Obsolete. Do <b>not</b> use this option anymore. To configure SNMP, see the <a href="#">R80.40 Gaia Administration Guide</a> - Chapter System Management - Section SNMP.
<b>PKCS#11 Token</b>	Register a cryptographic token, for use by Gaia Operating System. See details of the token, and test its functionality.
<b>Random Pool</b>	Configures the RSA keys, to be used by Gaia Operating System.
<b>Secure Internal Communication</b>	Manages SIC on the Security Gateway or Cluster Member. This change requires a restart of Check Point services on the Security Gateway or Cluster Member. For more information, see: <ul style="list-style-type: none"><li>■ The <a href="#">R80.40 Security Management Administration Guide</a>.</li><li>■ <a href="#">sk65764: How to reset SIC</a>.</li></ul>
<b>Enable cluster membership for this gateway</b>	Enables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the <a href="#">R80.40 ClusterXL Administration Guide</a> .
<b>Disable cluster membership for this gateway</b>	Disables the cluster membership on the Security Gateway. This change requires a reboot of the Security Gateway. For more information, see the <a href="#">R80.40 ClusterXL Administration Guide</a> .
<b>Enable Check Point Per Virtual System State</b>	Enables Virtual System Load Sharing on the VSX Cluster Member. For more information, see the <a href="#">R80.40 VSX Administration Guide</a> .

Menu Option	Description
<b>Disable Check Point Per Virtual System State</b>	<p>Disables Virtual System Load Sharing on the VSX Cluster Member.</p> <p>For more information, see the <a href="#">R80.40 VSX Administration Guide</a>.</p>
<b>Enable Check Point ClusterXL for Bridge Active/Standby</b>	<p>Enables Check Point ClusterXL for Bridge mode.</p> <p>This change requires a reboot of the Cluster Member.</p> <p>For more information, see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p>
<b>Disable Check Point ClusterXL for Bridge Active/Standby</b>	<p>Disables Check Point ClusterXL for Bridge mode.</p> <p>This change requires a reboot of the Cluster Member.</p> <p>For more information, see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p>
<b>Check Point CoreXL</b>	<p>Manages CoreXL on the Security Gateway or Cluster Member.</p> <p>After all changes in CoreXL configuration, you must reboot the Security Gateway or Cluster Member.</p> <p>For more information, see the <a href="#">R80.40 Performance Tuning Administration Guide</a>.</p>
<b>Automatic start of Check Point Products</b>	<p>Shows and controls which of the installed Check Point products start automatically during boot.</p>
<b>Exit</b>	<p>Exits from the Check Point Configuration Tool.</p>

# Installing Software Packages on Gaia

You can install Software Packages in these ways on Gaia R80.40:

## Installing Software Packages locally

You use the **CPUSE** on each Gaia computer to install the applicable packages.

For more information, see [sk92449](#).

- If a Gaia computer *is* connected to the Internet

Installation Method	Action Plan
Online	<ol style="list-style-type: none"> <li>1. Connect to the Gaia Portal or Gaia Clish on your Gaia computer.</li> <li>2. Verify the applicable CPUSE Software Packages.</li> <li>3. Download the applicable CPUSE Software Packages.</li> <li>4. Install the applicable CPUSE Software Packages.</li> </ol>
Offline	See the instructions for a Gaia computer that is <b>not</b> connected to the Internet.

- If a Gaia computer is **not** connected to the Internet

Installation Method	Action Plan
Offline only	<p><b>Installation in Gaia Portal</b></p> <ol style="list-style-type: none"> <li>1. Use the computer, from which you connect to Gaia Portal.</li> <li>2. Download the applicable CPUSE Software Packages from:           <ul style="list-style-type: none"> <li>• <a href="#">R80.40 Home Page</a></li> <li>• <a href="#">Upgrade Wizard</a></li> </ul> </li> <li>3. Connect to Gaia Portal on your Gaia computer.</li> <li>4. Import the applicable CPUSE Software Packages.</li> <li>5. Verify the applicable CPUSE Software Packages.</li> <li>6. Install the applicable CPUSE Software Packages.</li> </ol>

Installation Method	Action Plan
	<p><b>Installation in Gaia Clish</b></p> <ol style="list-style-type: none"> <li>1. Use the computer, from which you connect to Gaia Portal.</li> <li>2. Download the applicable CPUSE Software Packages from:           <ul style="list-style-type: none"> <li>• <a href="#">R80.40 Home Page</a></li> <li>• <a href="#">Upgrade Wizard</a></li> </ul> </li> <li>3. Transfer the applicable CPUSE Offline Software Packages to your Gaia computer to some directory (for example, <code>/var/log/path_to_CPUSE_packages/</code>).</li> <li>4. Connect to Gaia Clish on your Gaia computer.</li> <li>5. Import the applicable CPUSE Software Packages.</li> <li>6. Verify the applicable CPUSE Software Packages.</li> <li>7. Install the applicable CPUSE Software Packages.</li> </ol>



#### Important:

When you perform an upgrade to R80.40 with CPUSE from R80.20.M1, R80.20, R80.20.M2, or R80.30, you can see the upgrade report in Gaia Portal:

1. From the left navigation tree, click **Upgrades (CPUSE) > Status and Actions**.
2. In the **Major Versions** section, select the R80.40 Upgrade package.
3. In the right pane **Package Details**, click the link **To see a detailed upgrade report**.
4. A pop up opens and shows the upgrade progress in real time.

The report supports only these configurations:

- Security Management Servers
- Endpoint Security Management Servers
- CloudGuard Controllers
- Multi-Domain Servers
- Log Servers
- Endpoint Policy Servers
- Multi-Domain Log Servers
- Standalone Servers

## Installing Software Packages centrally

These options are available on an R80.40Management Server:

- Use the **Central Deployment** in SmartConsole to deploy the applicable packages to the managed Security Gateways and Clusters.

You can deploy a software package from:

- The Check Point Cloud.
- The Package Repository on the Management Server (first, you must upload the applicable package to the Package Repository).

For more information, see the [R80.40 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

**Best Practice - Best Practice - Use this method.**

- Use the **Central Deployment Tool** on the Management Server to deploy the applicable packages to the managed Security Gateways and Clusters.

For more information, see [sk111158](#).

# Upgrade Options and Prerequisites

This section contains the supported upgrade options and the upgrade prerequisites.



**Note** - You can use the [Upgrade/Download Wizard](#) to download the applicable installation and upgrade images.

# Prerequisites for Upgrading and Migrating of Management Servers and Log Servers

## Prerequisites:

- Make sure you use the latest version of this document (see the "*Important Information*" on page 3 page for links).
- See the [\*R80.40 Release Notes\*](#) for:
  - Supported upgrade paths
  - Minimum hardware and operating system requirements
  - Supported Security Gateways
- Make sure to read all applicable known limitations in the [R80.40 Known Limitations SK](#).
- When you use the **Advanced Upgrade** or the **Migration and Upgrade** method, before you import the management database on the R80.40 Servers, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#).

This makes sure the R80.40 Servers have the latest improvements for reported import issues.

This recommendation does not apply to the CPUSE Upgrade method, because these improvements are already integrated in R80.40 CPUSE Upgrade Package.

- **Licenses and Service Contracts:**

- Make sure you have valid licenses installed on all applicable Check Point computers - source and target.
- Make sure you have a valid Service Contract that includes software upgrades and major releases registered to your [Check Point User Center account](#).

The contract file is stored on the Management Server and downloaded to Check Point Security Gateways during the upgrade process.

For more information about Service Contracts, see [sk33089](#).

- If SmartConsole connects to the Management Server (which you plan to upgrade) through an R7x Security Gateway or Cluster, then follow the steps below.

## Procedure

1. Connect to the Management Server that manages the R7x Security Gateway or Cluster
2. Add a new explicit Firewall rule:

Source	Destination	VPN	Service	Action	Install On
SmartConsole Host object	Management Server object	Any Traffic	TCP 19009	Accept	R7x Security Gateway or Cluster

3. Install the modified Firewall Policy on the R7x Security Gateway or Cluster.

4. If later you upgrade this R7x Security Gateway or Cluster to R80.10 or higher, delete this explicit rule.
- On your Security Management Servers, Multi-Domain Servers, Domain Management Servers, Multi-Domain Log Servers, Domain Log Servers, Log Servers, and SmartEvent Servers:  
Make a copy of all custom configurations in the applicable directories and files.  
Pay special attention to these scripts:
    - \$CPDIR/tmp/.CPprofile.sh
    - \$CPDIR/tmp/.CPprofile.csh

The upgrade process replaces all existing files with default files. You must not copy the customized configuration files from the current version to the upgraded version, because these files can be unique for each version. You must make all the custom configurations again after the upgrade.

### List of the applicable directories

- \$FWDIR/lib/
- \$FWDIR/conf/
- \$CVPNDIR/conf/
- /opt/CP\*/lib/
- /opt/CP\*/conf/
- \$MDSDIR/conf/
- \$MDSDIR/customers/<Name\_of\_Domain>/CP\*/lib/
- \$MDSDIR/customers/<Name\_of\_Domain>/CP\*/conf/

- For your Management Servers in High Availability configuration, plan the upgrade.

### Action Plan for Security Management Servers in High Availability



**Important** - To back up and restore a consistent Security Management environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.

Upgrade to R80.40	Action Plan
From R80, R80.10, R80.20, R80.20.M2, and higher versions	<ol style="list-style-type: none"> <li>1. Upgrade the Primary Security Management Server.</li> <li>2. Upgrade the Secondary Security Management Servers.</li> </ol>
From R7X or R80.20.M1 versions	<ol style="list-style-type: none"> <li>1. Upgrade the Primary Security Management Server.</li> <li>2. Perform a clean install of the Secondary Security Management Servers.</li> <li>3. Connect the Secondary Security Management Servers to the Primary Security Management Server.</li> </ol>

## Action Plan for Multi-Domain Servers in High Availability



**Important** - To back up and restore a consistent Multi-Domain Security Management environment, make sure to collect and restore the backups and snapshots from all servers in the High Availability environment at the same time.

Upgrade to R80.40	Action Plan
From R80.20, R80.20.M2, and higher versions	<ol style="list-style-type: none"> <li>1. <b>Make sure to run Pre-Upgrade Verifier on all source servers and to fix all detected issues before you start the upgrade.</b></li> <li>2. Make sure the Global Domain is Active on the Primary Multi-Domain Server.</li> <li>3. Upgrade the Primary Multi-Domain Server.</li> <li>4. Upgrade the Secondary Multi-Domain Servers.</li> </ol>
From R80.20.M1 version	<ol style="list-style-type: none"> <li>1. <b>Make sure to run Pre-Upgrade Verifier on all source servers and to fix all detected issues before you start the upgrade.</b></li> <li>2. Make sure the Global Domain is Active on the Primary Multi-Domain Server.</li> <li>3. Upgrade the Primary Multi-Domain Server.</li> <li>4. Perform a clean install of the Secondary Multi-Domain Servers.</li> <li>5. Connect the Secondary Multi-Domain Servers to the Primary Multi-Domain Server.</li> </ol>
From R7X or R80.10 versions	<ul style="list-style-type: none"> <li>• If the Primary Multi-Domain Server is not available at this time, you must first promote the Secondary Multi-Domain Server to be the Primary.</li> </ul>

- If your Security Management Server or Multi-Domain Server manages dedicated Log Servers or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Management Server.



**Important** - You must upgrade your Management Servers before you can upgrade these dedicated servers.



**Note** - SmartEvent Server can run the same version or higher than the Log Server.

- If your Multi-Domain Server manages Multi-Domain Log Servers, you must upgrade the Multi-Domain Log Servers to the same version as the Multi-Domain Server.



**Important** - You must upgrade your Multi-Domain Servers before you can upgrade the Multi-Domain Log Servers.

- Before you upgrade a Multi-Domain Server, we recommend the steps below to optimize the upgrade process.

## Procedure

Step	Instructions
1	<p>Delete all unused Threat Prevention Profiles on the Global Domain:</p> <p>On R80.x Multi-Domain Server:</p> <ol style="list-style-type: none"> <li>Connect with SmartConsole to the Global Domain.</li> <li>From the left navigation panel, click <b>Security Policies</b>.</li> <li>Open every policy.</li> <li>In the top section, click <b>Threat Prevention</b>.</li> <li>In the bottom section <b>Threat Tools</b>, click <b>Profiles</b>.</li> <li>Delete all unused Threat Prevention Profiles.</li> <li>Publish the SmartConsole session.</li> <li>Close SmartConsole.</li> </ol> <p>On R77.x Multi-Domain Server:</p> <ol style="list-style-type: none"> <li>Connect with SmartDashboard to the Global Domain.</li> <li>Go to <b>Threat Prevention</b> tab.</li> <li>From the left tree, click <b>Profiles</b>.</li> <li>Delete all unused Threat Prevention Profiles.</li> <li>Save the changes (click <b>File &gt; Save</b>).</li> <li>Close SmartDashboard.</li> </ol>
2	<p>Disable the Staging Mode for IPS protections (see <a href="#">sk142432</a>):</p> <ol style="list-style-type: none"> <li>Connect with SmartConsole to every Domain.</li> <li>From the left navigation panel, click <b>Security Policies</b>.</li> <li>Open every policy.</li> <li>In the top section, click <b>Threat Prevention</b>.</li> <li>In the bottom section <b>Threat Tools</b>, click <b>Profiles</b>.</li> <li>Edit every profile.</li> <li>From the left tree, click <b>IPS &gt; Updates</b>.</li> <li>Clear the box <b>Set activation as staging mode (Detect)</b>.</li> <li>Click <b>OK</b>.</li> <li>Publish the SmartConsole session.</li> <li>Close SmartConsole.</li> </ol>

- Before you start an upgrade or migration procedure on your Management Servers, you must close all GUI clients (SmartConsole applications) connected to your Check Point computers.
- Before you start an upgrade of your Security Gateway and Cluster Members, you must upgrade the Management Server.
- On Smart-1 appliances with Multi-Domain Server or Multi-Domain Log Server installed, if you configured an interface other than **Mgmt** as the Leading interface, the upgrade process or clean install process (with CPUSE) configures the interface **Mgmt** to be the Leading interface. To configure another interface as the Leading interface after the upgrade, see [sk107336](#).

**Required Disk Space:**

- The size of the `/var/log/` partition on the target Management Server or Log Server must be at least 25% of the size of the `/var/log/` partition on the source Management Server or Log Server.
- For Advanced Upgrade or Migration procedure, the hard disk on the Management Server or Log Server must be at least 5 times the size of the exported database.

**IPv4 or IPv6 Addresses:**

If the source Security Management Server uses only IPv4 or only IPv6, the target Security Management Server must use the same IP address configuration. You can change this configuration later, after the upgrade or migration, if needed.

# Prerequisites for Upgrading and Migrating of Security Gateways and Clusters

## Prerequisites:

- Make sure you use the latest version of this document (see the "*Important Information*" on page 3 page for links).
- See the [\*R80.40 Release Notes\*](#) for:
  - Supported upgrade paths
  - Minimum hardware and operating system requirements
  - Supported Security Gateways
- Make sure to read all applicable known limitations in the [R80.40 Known Limitations SK](#).
- Before starting an upgrade of your Security Gateway and Cluster Members, you must upgrade the Management Server.
- On your Security Gateways and Cluster Members:

Make a copy of all custom configurations in the applicable directories and files.

The upgrade process replaces all existing files with default files. You must not copy the customized configuration files from the current version to the upgraded version, because these files can be unique for each version. You must make all the custom configurations again after the upgrade.

## List of the most important directories



**Note** - On VSX Gateway and VSX Cluster Member, some of these directories exist in the context of each Virtual Device.

- \$FWDIR/boot/modules/
- \$FWDIR/conf/
- \$FWDIR/lib/
- \$FWDIR/database/
- \$CVPNDIR/conf/
- \$PPKDIR/boot/modules/
- /var/ace/

## List of the most important files



**Note** - Some of these files do not exist by default. Some files are configured on each VSX Gateway and VSX Cluster Member, and some files are configured for each Virtual System.

- \$FWDIR/boot/modules/fwkern.conf
- \$FWDIR/boot/modules/vpnkern.conf

- \$FWDIR/conf/fwaffinity.conf
- \$FWDIR/conf/fwauthd.conf
- \$FWDIR/conf/local.arp
- \$FWDIR/conf/disctnd.if
- \$FWDIR/conf/cpha\_bond\_ls\_config.conf
- \$FWDIR/conf/resctrl
- \$FWDIR/conf/vsaffinity\_exception.conf
- \$FWDIR/database/qos\_policy.C
- simkern.conf:
  - In R80.20 and higher: \$PPKDIR/conf/simkern.conf
  - In R80.10 and lower: \$PPKDIR/boot/modules/simkern.conf
- sim\_aff.conf:
  - In R80.20 and higher: \$PPKDIR/conf/sim\_aff.conf
  - In R80.10 and lower: \$PPKDIR/boot/modules/sim\_aff.conf
- \$CPDIR/tmp/.CPprofile.sh
- \$CPDIR/tmp/.CPprofile.csh
- /var/ace/sdconf.rec
- /var/ace/sdopts.rec
- /var/ace/sdstatus.12
- /var/ace/securid

### List of the most important files



**Note** - Some of these files do not exist by default. Some files are configured on each VSX Gateway and VSX Cluster Member, and some files are configured for each Virtual System.

- \$FWDIR/boot/modules/fwkern.conf
- \$FWDIR/boot/modules/vpnkern.conf
- \$FWDIR/conf/fwaffinity.conf
- \$FWDIR/conf/fwauthd.conf
- \$FWDIR/conf/local.arp
- \$FWDIR/conf/disctnd.if
- \$FWDIR/conf/cpha\_bond\_ls\_config.conf
- \$FWDIR/conf/resctrl
- \$FWDIR/conf/vsaffinity\_exception.conf
- \$FWDIR/database/qos\_policy.C

- simkern.conf:
  - In R80.20 and higher: \$PPKDIR/conf/simkern.conf
  - In R80.10 and lower: \$PPKDIR/boot/modules/simkern.conf
- sim\_aff.conf:
  - In R80.20 and higher: \$PPKDIR/conf/sim\_aff.conf
  - In R80.10 and lower: \$PPKDIR/boot/modules/sim\_aff.conf
- /var/ace/sdconf.rec
- /var/ace/sdopts.rec
- /var/ace/sdstatus.12
- /var/ace/securid

■ **Licenses and Service Contracts:**

- Make sure you have valid licenses installed on all applicable Check Point computers - source and target.
- Make sure you have a valid Service Contract that includes software upgrades and major releases registered to your [Check Point User Center account](#).

The contract file is stored on the Management Server and downloaded to Check Point Security Gateways during the upgrade process.

For more information about Service Contracts, see [sk33089](#).

# Prerequisites for Upgrading the Mobile Access Software Blade Configuration



**Important** - If you use the Mobile Access Software Blade and you have customized configuration, review the customized settings **before** you upgrade to R80.40. Do **not** copy the existing files, because the default files change between the versions. After the upgrade, make the applicable changes to the new files.

## Prerequisites:

- Make sure you use the latest version of this document (see the "*Important Information*" on page 3 page for links).
- See the [R80.40 Release Notes](#) for:
  - Supported upgrade paths
  - Minimum hardware and operating system requirements
  - Supported Security Gateways
- Make sure to read all applicable known limitations in the [R80.40 Known Limitations SK](#).
- Before starting an upgrade of your Security Gateway and Cluster Members, you must upgrade the Management Server.
- **Licenses and Service Contracts:**
  - Make sure you have valid licenses installed on all applicable Check Point computers - source and target.
  - Make sure you have a valid Service Contract that includes software upgrades and major releases registered to your [Check Point User Center account](#).

The contract file is stored on the Management Server and downloaded to Check Point Security Gateways during the upgrade process.

For more information about Service Contracts, see [sk33089](#).

## Procedure:

Step	Instructions
1	<p>Open these files on the Management Server and write down all custom changes in the applicable files:</p> <ul style="list-style-type: none"> <li>■ Mobile Access configuration: \$CVPNDIR/conf/cvpnd.C</li> <li>■ Apache configuration: \$CVPNDIR/conf/httpd.conf \$CVPNDIR/conf/includes/*</li> <li>■ Local certificates: \$CVPNDIR/var/ssl/ca-bundle/*</li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>■ DynamicID - SMS OTP - Local Phone List: \$CVPNDIR/conf/SmsPhones.lst</li> <li>■ RSA configuration: /var/ace/sdconf.rec</li> <li>■ Mobile Access Gaia Portal configuration (run these commands in the Expert mode to see the applicable files):           <pre>find \$CVPNDIR/ -name *.php -type f -exec ls {} \; find \$CVPNDIR/ -name *.gif -type f -exec ls {} \; find \$CVPNDIR/ -name *.jpg -type f -exec ls {} \;</pre> </li> </ul>
2	Upgrade the Management Server to R80.40 using one of the supported methods (see " <a href="#">Upgrade Methods</a> " on page 175).
3	<p>Update the Mobile Access Endpoint Compliance:</p> <ol style="list-style-type: none"> <li>1. In SmartConsole, from the left navigation panel, click <b>Security Policies</b>.</li> <li>2. In the <b>Shared Policies</b> section, click <b>Mobile Access</b> &gt; Open <b>Mobile Access Policy in SmartDashboard</b>.</li> <li>3. In SmartDashboard, click <b>Mobile Access</b> tab &gt; open <b>Endpoint Security on Demand</b> &gt; click <b>Endpoint Compliance Updates</b> &gt; click <b>Update Databases Now</b>.</li> <li>4. Close SmartDashboard.</li> </ol>
4	Manually edit the default files on the upgraded the Management Server to include your custom changes.

# Prerequisites for Upgrading vSEC Controller R80.10 and lower

## Important Information:

Step	Instructions
1	See the Known Limitation VSECPC-1341 in <a href="#">sk122486</a> .
2	See the <a href="#">R80.40 CloudGuard Controller Administration Guide</a> for a list of supported Security Gateways.
3	When you upgrade a vSEC Controller R80.10 and lower to CloudGuard Controller R80.40, these files are overwritten with default values: <ul style="list-style-type: none"> <li>■ \$MDS_FWDIR/conf/vsec.conf</li> <li>■ \$MDS_FWDIR/conf/tagger_db.C</li> <li>■ \$MDS_FWDIR/conf/AWS_regions.conf</li> </ul> Before you begin the upgrade, back up all files you changed in the past.
4	Before you begin the upgrade on a vSEC Controller R80.10 and lower, if you have a Cisco APIC server, keep only one URL. After the upgrade, add the other URLs.



**Note** - During the upgrade, vSEC Controller R80.10 and lower does not communicate with the Data Centers. Therefore, Data Center objects are not updated on the vSEC Controller or the Security Gateways.

## Licenses and Service Contracts

- Make sure you have valid licenses installed on all applicable Check Point computers - source and target.
- Make sure you have a valid Service Contract that includes software upgrades and major releases registered to your [Check Point User Center account](#).

The contract file is stored on the Management Server and downloaded to Check Point Security Gateways during the upgrade process.

For more information about Service Contracts, see [sk33089](#).

# Upgrade Methods

You can use this method to upgrade your Security Gateways and Cluster Members:

Gateway	Central Deployment Tool	CPUSE
Security Gateways, VSX Gateways, Cluster Members	See " <a href="#">Upgrade of Security Gateways and Cluster Members with Central Deployment Tool</a> " on the next page	See " <a href="#">Upgrade with CPUSE</a> " on the next page

You can use these methods to upgrade your Management Servers and Log Servers:

Server	CPUSE	Advanced Upgrade	Migration and Upgrade	Gradual Upgrade
Security Management Server, Endpoint Security Management Server, CloudGuard Controller, vSEC Controller	See " <a href="#">Upgrade with CPUSE</a> " on the next page	See " <a href="#">Advanced Upgrade of Management Servers and Log Servers</a> " on page 177	See " <a href="#">Migration and Upgrade of Management Servers and Log Servers</a> " on page 178	N / A
Multi-Domain Server	See " <a href="#">Upgrade with CPUSE</a> " on the next page	See " <a href="#">Advanced Upgrade of Management Servers and Log Servers</a> " on page 177	See " <a href="#">Migration and Upgrade of Management Servers and Log Servers</a> " on page 178	See " <a href="#">Gradual Upgrade of an R7x Multi-Domain Server</a> " on page 179
Multi-Domain Log Server	See " <a href="#">Upgrade with CPUSE</a> " on the next page	See " <a href="#">Advanced Upgrade of Management Servers and Log Servers</a> " on page 177	See " <a href="#">Migration and Upgrade of Management Servers and Log Servers</a> " on page 178	N / A
Dedicated Log Server, Endpoint Policy Server	See " <a href="#">Upgrade with CPUSE</a> " on the next page	See " <a href="#">Advanced Upgrade of Management Servers and Log Servers</a> " on page 177	See " <a href="#">Migration and Upgrade of Management Servers and Log Servers</a> " on page 178	N / A

Server	CPUSE	Advanced Upgrade	Migration and Upgrade	Gradual Upgrade
Dedicated SmartEvent Server	See " <a href="#">Upgrade with CPUSE below</a> "	See " <a href="#">Advanced Upgrade of Management Servers and Log Servers</a> " on the next page	See " <a href="#">Migration and Upgrade of Management Servers and Log Servers</a> " on page 178	N / A

**Important:**

- Upgrade with CPUSE is supported only on Check Point computers that currently run Gaia Operating System.
- Before you upgrade your Security Gateways and Cluster Members, you must upgrade your Management Servers that manage them.
- You must upgrade your dedicated Log Servers and SmartEvent Servers to the same version as the Management Servers that manage them.  
You must upgrade your Management Servers before you can upgrade these dedicated servers.
- You must upgrade your Multi-Domain Log Servers to the same version as the Multi-Domain Servers that manage them.
- Gradual Upgrade is supported only from R7x versions.
- During the upgrade process in a Management High Availability environment, we recommend that you do **not** use **any** of the Security Management Servers or Multi-Domain Servers to make changes in the management databases.  
This can cause inconsistent synchronization between these servers.

**Upgrade of Security Gateways and Cluster Members with Central Deployment Tool**

With Central Deployment Tool on the Management Server, you can install software packages to upgrade or to perform a clean install on Security Gateways and Cluster Members.

For more information, see [sk111158](#).

**Upgrade with CPUSE**

With CPUSE, you can install software packages to upgrade or to perform a clean install on Check Point computers that run on the Gaia Operating System.

For more about CPUSE, see [sk92449](#).

For detailed CPUSE upgrade instructions, see:

Upgrade From	Section in this Guide
R80.30, R80.20.M2, R80.20, R80.20.M1	<ul style="list-style-type: none"> <li>■ "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE</a>" on page 245</li> <li>■ "<a href="#">Upgrading one Multi-Domain Server from R80.20 and higher</a>" on page 305</li> <li>■ "<a href="#">Upgrading Multi-Domain Servers in High Availability from R80.20 and higher</a>" on page 358</li> <li>■ "<a href="#">Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE</a>" on page 431</li> <li>■ "<a href="#">Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE</a>" on page 500</li> </ul>
R80.10 and lower	<ul style="list-style-type: none"> <li>■ "<a href="#">Upgrading a Security Management Server from R80.10 and lower with CPUSE</a>" on page 187</li> <li>■ "<a href="#">Upgrading an Endpoint Security Management Server from R80.10 and lower with CPUSE</a>" on page 457</li> <li>■ "<a href="#">Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with CPUSE</a>" on page 483</li> <li>■ "<a href="#">Upgrading a Dedicated Log Server from R80.10 and lower with CPUSE</a>" on page 213</li> <li>■ "<a href="#">Upgrading a Dedicated SmartEvent Server from R80.10 and lower with CPUSE</a>" on page 229</li> <li>■ "<a href="#">Upgrading one Multi-Domain Server from R80.10 and lower</a>" on page 272</li> <li>■ "<a href="#">Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with CPUSE</a>" on page 324</li> <li>■ "<a href="#">Upgrading a Multi-Domain Log Server from R80.10 and lower with CPUSE</a>" on page 410</li> <li>■ "<a href="#">Upgrading a Security Gateway with CPUSE</a>" on page 527</li> <li>■ "<a href="#">Upgrading a VSX Gateway with CPUSE</a>" on page 531</li> </ul>



**Note** - When you perform an upgrade to R80.40 with CPUSE from R80.20.M1, R80.20, R80.20.M2, or R80.30, you can see the upgrade report in Gaia Portal. See "[Installing Software Packages on Gaia](#)" on page 160.

## Advanced Upgrade of Management Servers and Log Servers

In an advanced upgrade scenario, perform these steps on the same Check Point computer:

Step	Instructions
1	Take a full backup and snapshot of the current Check Point computer.
2	Export the entire management database with the R80.40 Management Server Migration Tool.
3	Get the R80.40 Check Point computer: <ul style="list-style-type: none"> <li>■ If the current Check Point computer runs on Gaia, you can upgrade it to R80.40.</li> <li>■ If the current Check Point computer runs an operating system other than Gaia, you must perform a clean install of the R80.40.</li> </ul>
4	Import the entire management database.

For detailed Advanced Upgrade instructions, see:

Upgrade From	Section in this Guide
R80.30, R80.20.M2, R80.20, R80.20.M1	<ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 250</a></li> <li>■ <a href="#">"Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade" on page 309</a></li> <li>■ <a href="#">"Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade" on page 366</a></li> <li>■ <a href="#">"Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade" on page 437</a></li> <li>■ <a href="#">"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade" on page 505</a></li> </ul>
R80.10 and lower	<ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading a Security Management Server from R80.10 and lower with Advanced Upgrade" on page 190</a></li> <li>■ <a href="#">"Upgrading an Endpoint Security Management Server from R80.10 and lower with Advanced Upgrade" on page 460</a></li> <li>■ <a href="#">"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Advanced Upgrade" on page 487</a></li> <li>■ <a href="#">"Upgrading a Dedicated Log Server from R80.10 and lower with Advanced Upgrade" on page 216</a></li> <li>■ <a href="#">"Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Advanced Upgrade" on page 232</a></li> <li>■ <a href="#">"Upgrading one Multi-Domain Server from R80.10 and lower with Advanced Upgrade" on page 277</a></li> <li>■ <a href="#">"Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Advanced Upgrade" on page 329</a></li> <li>■ <a href="#">"Upgrading a Multi-Domain Log Server from R80.10 and lower with Advanced Upgrade" on page 414</a></li> </ul>



**Note** - When you perform an upgrade to R80.40 from R80.20.M1, R80.20, R80.20.M2, or R80.30, you can see the upgrade report on the server. The upgrade process generates this report after each specific stage of an upgrade:  
`$MDS_FWDIR/log/upgrade_report-<yyyy.MM.dd.HH.mm.ss>.html`

## Migration and Upgrade of Management Servers and Log Servers

In a migration and upgrade scenario, perform these steps on the source Check Point computer and the different target Check Point computer:

Step	Instructions
1	Export the entire management database from the source Check Point computer with the R80.40 Management Server Migration Tool.
2	Install another target R80.40 Check Point computer.
3	Import the entire management database on the new target R80.40 Check Point computer.

For detailed migration and upgrade instructions, see:

Upgrade From	Section
R80.30, R80.20.M2, R80.20, R80.20.M1	<ul style="list-style-type: none"> <li>■ "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration</a>" on page 259</li> <li>■ "<a href="#">Upgrading one Multi-Domain Server from R80.20 and higher with Migration</a>" on page 316</li> <li>■ "<a href="#">Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration</a>" on page 387</li> <li>■ "<a href="#">Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration</a>" on page 446</li> <li>■ "<a href="#">Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration</a>" on page 513</li> </ul>
R80.10 and lower	<ul style="list-style-type: none"> <li>■ "<a href="#">Upgrading a Security Management Server from R80.10 and lower with Migration</a>" on page 200</li> <li>■ "<a href="#">Upgrading an Endpoint Security Management Server from R80.10 and lower with Migration</a>" on page 470</li> <li>■ "<a href="#">Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Migration</a>" on page 493</li> <li>■ "<a href="#">Upgrading a Dedicated Log Server from R80.10 and lower with Migration</a>" on page 222</li> <li>■ "<a href="#">Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Migration</a>" on page 238</li> <li>■ "<a href="#">Upgrading one Multi-Domain Server from R80.10 and lower with Migration</a>" on page 285</li> <li>■ "<a href="#">Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Migration</a>" on page 343</li> <li>■ "<a href="#">Upgrading a Multi-Domain Log Server from R80.10 and lower with Migration</a>" on page 422</li> </ul>



**Note** - When you perform an upgrade to R80.40 from R80.20.M1, R80.20, R80.20.M2, or R80.30, you can see the upgrade report on the target server. The upgrade process generates this report after each specific stage of an upgrade:  
`$MDS_FWDIR/log/upgrade_report-<yyyy.MM.dd_HH.mm.ss>.html`

## Gradual Upgrade of an R7x Multi-Domain Server

In a gradual scenario, perform these steps on the source R7x Multi-Domain Server and the target R80.40 Multi-Domain Server:

Step	Instructions
1	Install a target R80.40 Multi-Domain Server.
2	Create the corresponding Domain Management Servers, into which you import the entire management databases from the source R7x Domain Management Servers.
3	Migrate the Global Policy from the current R7x Multi-Domain Server to the R80.40 Multi-Domain Server.

Step	Instructions
4	On the current R7x Multi-Domain Server, export the entire management databases from the applicable source R7x Domain Management Servers one by one with the R80.40 Management Server Migration Tool.
5	On the target R80.40 Multi-Domain Server, import the entire management databases to the applicable target R80.40 Domain Management Servers one by one.



**Best Practice** - We recommend you upgrade the entire Multi-Domain Server at once.

For detailed gradual upgrade instructions, see "["Upgrading one R7x Multi-Domain Server with Gradual Migration of Domain Management Servers" on page 293.](#)

# Contract Verification

Before you upgrade your Management Server to R80.40, you must have a valid Support Contract that includes software upgrades and major releases registered to your Check Point User Center account.

By verifying your status with the User Center, the contract file enables you to remain compliant with current Check Point licensing standards.

As in all upgrade procedures, first upgrade your Security Management Server or Multi-Domain Server before upgrading the Security Gateways.

When you upgrade a Management Server, the upgrade process checks to see whether a Contract File is already present.

If a Contract File is not present, later you can download a Contract File manually from the Check Point User Center and import it.

If a Contract File does not cover the Management Server, a message informs you that the Management Server is not eligible for upgrade.



**Important** - The absence of a valid Contract File does **not** prevent upgrade.



**Note** - In most cases, you do **not** need to worry about your Service Contract File. Your Management Server is configured to communicate with the User Center automatically, and download the most current file. This allows the Management Server to enable the purchased services properly.

You can download a valid Contract File later.

Option	Instructions
Download a contract file from the User Center	If you have Internet access and a valid <a href="#">Check Point User Center</a> account, download a Contract File directly from your User Center account:
Import a local contract file	<p>If the Management Server does not have Internet access:</p> <ol style="list-style-type: none"> <li>On a computer with Internet access, log in to your <a href="#">Check Point User Center</a> account.</li> <li>In the top menu, click <b>Assets/Info &gt; Download Contract File</b> and follow the instructions on the screen.</li> <li>Transfer the downloaded contract file to your Management Server.</li> <li>Select <b>Import a local contracts file</b>.</li> <li>Enter the full path to the location where you stored the contract file.</li> </ol>
Continue without contract information	<p>Select this option, if you intend to get and install a valid Contract File later. Note that at this point your managed Security Gateways are not strictly eligible for an upgrade.</p> <p>You may be in violation of your Check Point Licensing Agreement, as shown in the final message of the upgrade process.</p>

# Management Server Migration Tool and Upgrade Tools

## Important:



- You must always use the latest version of the R80.40 Upgrade Tools from [sk135172](#) to:
  - Upgrade from R80.20.M1, R80.20, R80.20.M2, or R80.30
  - Migrate a Domain Management Server between Multi-Domain Servers
  - Migrate a Domain Management Server from a Multi-Domain Server to a Security Management Server
  - Migrate a Security Management Server to a Domain on a Multi-Domain Server
  - Back up and restore a Domain on a Multi-Domain Server

## Notes:

- If the Management Server / Log Server is connected to the Internet and you enabled the "Allow Download" consent flag (see [sk111080](#)), then the server downloads and installs the latest version of the Upgrade Tools automatically.

To enable the "Allow Download" consent flag:

- In the Gaia First Time Configuration Wizard, you selected the option **Automatically download Blade Contracts, new software, and other important data**.
- In SmartConsole, you selected the option **Automatically download Contracts and other important data** in **Menu > Global properties > Security Management**.
- If the Management Server / Log Server is not connected to the Internet, then you must install the latest version of the Upgrade Tools manually.

- To upgrade from R80.10 and lower, you must always use the Management Server Migration Tool of the version, to which you upgrade.

Download the applicable Management Server Migration Tool package from the [R80.40 Home Page](#)

These Upgrade Tools:

- Make sure it is possible to upgrade the current management database without issues.
- Generate an upgrade report with the list of detected issues that can fail the upgrade.

The upgrade report shows these messages:

Message Category	Instructions
Action items before the upgrade	Errors you must repair before the upgrade. Warnings of issues for you to decide whether to fix before upgrade. An example of an error you must fix before the upgrade is an invalid policy name.
Action items after the upgrade	Errors and warnings that you must fix after the upgrade.
Information messages	Items to be aware of. For example, an object type is not supported in the higher version, but is in your database and it is converted during the upgrade.

The most important files in the Management Server Migration Tool and Upgrade Tools packages:

Package	Instructions
migrate migrate_server	Exports and imports the management database and applicable Check Point configuration. For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> : <ul style="list-style-type: none"><li>■ Section <i>migrate</i>.</li><li>■ Section <i>migrate_server</i>.</li></ul>
migrate.conf	Contains configuration settings for Advanced Upgrade / Database Migration.
ips_upgrade_tool	Runs the IPS database upgrade.
pre_upgrade_verifier	Analyzes compatibility of the currently installed configuration with the version, to which you upgrade. It gives a report on the actions to take before and after the upgrade.   <b>Note</b> - This tool is required only when you upgrade from R77.30 (and lower) version.
puv_report_generator	Runs at the end of <code>pre_upgrade_verifier</code> and converts the text report file to an HTML file.   <b>Note</b> - This tool is required only when you upgrade from R77.30 (and lower) version.

## Using the Pre-Upgrade Verifier



**Best Practice** - Always run the Pre-Upgrade Verifier (PUV) on the source server before the upgrade.

The Pre-Upgrade Verifier:

- Analyzes compatibility of the currently installed configuration with the version, to which you upgrade. It gives a report on the actions to take before and after the upgrade.
- Can only analyze a management database that is intended for upgrade to a different major version (for example, from R80.20 to R80.40).
- Runs automatically during the upgrade process. You can also run it manually.

Run this command and use the applicable syntax based on the instructions on the screen:

Version	Server	Commands
R80.20 and higher	Security Management Server	<pre>\$FWDIR/scripts/migrate_server -h</pre>
	Multi-Domain Server, Multi-Domain Log Server	<pre>\$MDS_FWDIR/scripts/migrate_server verify -h</pre>
R80.10 and lower	Security Management Server	<pre>cd /&lt;Path to Extracted Migration Tool&gt;/ . /pre_upgrade_verifier -h</pre>
	Multi-Domain Server, Multi-Domain Log Server	<pre>mount -o loop /var/log/path_to_ iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom cd /mnt/cdrom/linux/p1_install/ . /mds_setup</pre> <p>Select this option: (1) Run Pre-upgrade verification only</p>

# Upgrade of Security Management Servers and Log Servers

This section provides instructions to upgrade Security Management Servers and Log Servers:

- "[Upgrading a Security Management Server or vSEC Controller from R80.10 and lower](#)" on page 186
- "[Upgrading a Dedicated Log Server from R80.10 and lower](#)" on page 212
- "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower](#)" on page 228
- "[Upgrading a Security Management Server or Log Server from R80.20 and higher](#)" on page 244

# Upgrading a Security Management Server or vSEC Controller from R80.10 and lower

This section provides instructions to upgrade Security Management Servers, Endpoint Security Management Server, or vSEC Controller R80.10 and lower:

- [\*"Upgrading a Security Management Server from R80.10 and lower with CPUSE" on page 187\*](#)
- [\*"Upgrading a Security Management Server from R80.10 and lower with Advanced Upgrade" on page 190\*](#)
- [\*"Upgrading a Security Management Server from R80.10 and lower with Migration" on page 200\*](#)
- [\*"Upgrading Security Management Servers in Management High Availability from R80.10 and lower" on page 207\*](#)

# Upgrading a Security Management Server from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Security Management Server.

**Notes:**



- To upgrade from R80.20 and higher, see "[Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE](#)" on page 245.
- This upgrade method is supported only for servers that already run on Gaia Operating System.
- These instructions equally apply to:
  - Security Management Server
  - vSEC Controller R80.10 and lower

**Important - Before you upgrade a Security Management Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

**Procedure:****1. Upgrade the Security Management Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**2. Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on page 89.

**3. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers**

If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Security Management Server:

- "[Upgrading a Dedicated Log Server from R80.10 and lower](#)" on page 212
- "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower](#)" on page 228

**4. Install the management database**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**5. Install the Event Policy**

**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .

Step	Instructions
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 6. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <code>cp_log_export reconf</code>
4	Restart the Log Exporter: <code>cp_log_export restart</code>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter *Log Exporter*.

## 7. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Security Management Server from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Security Management Server.

**Notes:**



- To upgrade from R80.20 and higher, see "["Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 250](#)".
- These instructions equally apply to:
  - Security Management Server
  - vSEC Controller R80.10 and lower

**Important - Before you upgrade a Security Management Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current Security Management Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Security Management Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p> <b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Security Management Server, then export the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the current Security Management Server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install the R80.40 Security Management Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading a Security Management Server or vSEC Controller from R80.10 and lower" on page 186</a></li> <li>■ <a href="#">"Installing a Security Management Server" on page 61</a></li> </ul>
Operating System other than Gaia	<p>Follow this procedure:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing a Security Management Server" on page 61</a></li> </ul>

**Important:**

- If you upgrade from R80 (or higher) version to R80.40, then these options are available:
  - The IP addresses of the source and target Security Management Servers **can be the same**.  
If in the future it is necessary to have a different IP address on the R80.40 Security Management Server, you can change it. For applicable procedures, see [sk40993](#) and [sk65451](#).  
Note that you have to issue licenses for the new IP address.
  - The IP addresses of the source and target Security Management Servers **can be different**.  
Note that you have to issue licenses for the new IP address.  
You must install the new licenses only after you import the databases.
- If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Security Management Servers **must be the same**.  
If it is necessary to have a different IP address on the R80.40 Security Management Server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.

**4. On the R80.40 Security Management Server, import the databases**

**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Security Management Server.
2	Log in to the Expert mode.
3	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> If it is not already installed, then install a valid license now.
4	Transfer the exported databases from an external storage to the R80.40 Security Management Server, to some directory. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <b>Note</b> - Make sure to transfer the files in the binary mode.         </div>
5	Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Security Management Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> </div>
6	Go to the \$FWDIR/bin/upgrade_tools/ directory: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cd \$FWDIR/bin/upgrade_tools/</pre> </div>

Step	Instructions
7	<p>Import the management database:</p> <pre data-bbox="441 271 1287 339">yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ If you upgrade from R80 (or higher) version, and the IP addresses of the source and target Security Management Servers <b>are different</b>:       <ol style="list-style-type: none"> <li>a. Issue licenses for the new IP address in your Check Point User Center account.</li> <li>b. Install the new licenses on the R80.40 Security Management Server.</li> </ol> </li> <li>■ If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Security Management Servers <b>must be the same</b>.       <ul style="list-style-type: none"> <li>• If it is necessary to have a different IP address on the R80.40 Security Management Server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.</li> </ul> </li> </ul>
8	 <p><b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Security Management Server, then import the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
9	<p>Restart the Check Point services:</p> <pre data-bbox="441 1417 557 1484">cpstop cpstart</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Install the licenses and change the IP address of the R80.40 Security Management Server

Scenario	Instructions
You upgraded from R80 (or higher) version to R80.40, and the IP addresses of the source and target Security Management Servers <b>are different</b>	<p>Follow these steps:</p> <ol style="list-style-type: none"><li data-bbox="965 271 1441 361">Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.</li><li data-bbox="965 372 1394 462">Install the new licenses on the R80.40 Security Management Server.</li></ol>

Scenario	Instructions
<p>You upgraded from R77.30 (and lower) version to R80.40 and need to have a different IP address on the R80.40 Security Management Server</p>	<p>Follow these steps (based on <a href="#">sk40993</a>):</p> <ul style="list-style-type: none"> <li>a. Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.</li> <li>b. Perform the required changes in the SmartConsole: <ul style="list-style-type: none"> <li>i. Connect with SmartConsole to the Security Management Server.</li> <li>ii. From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>iii. Open the Security Management Server object.</li> <li>iv. On the <b>General Properties</b> page, change the current IP address to the new IP address.</li> <li>v. On the <b>Network Management</b> page, edit the applicable interface and change the current IP address to the new IP address.</li> <li>vi. Click <b>OK</b>.</li> <li>vii. Publish the SmartConsole session.</li> <li>viii. Close the SmartConsole.</li> </ul> </li> <li>c. Stop the Check Point services: <ul style="list-style-type: none"> <li>i. Connect to the command line.</li> <li>ii. Log in to either Gaia Clish, or Expert mode.</li> <li>iii. Run: <code>cpstop</code></li> </ul> </li> <li>d. Perform the required changes in Gaia OS: <ul style="list-style-type: none"> <li>i. Connect to either Gaia Portal, or Gaia Clish.</li> <li>ii. Edit the applicable interface and change the current IP address to the new IP address.</li> </ul> </li> </ul> <p>You can perform this change in either Gaia Portal, or Gaia Clish. For details, see <a href="#">R80.40 Gaia Administration Guide</a>.</p>

Scenario	Instructions
	 <b>Note</b> - If this Security Management Server has only one interface, then your HTTPS and SSH connection to this Security Management Server is interrupted when you change its IP address. You need to connect again. To avoid this interruption, connect to the Security Management Server over the serial console. <ol style="list-style-type: none"> <li data-bbox="970 698 1383 799">e. Install the new licenses on the R80.40 Security Management Server.</li> <li data-bbox="1002 799 1430 911">You can do this either in the CLI with the "cplic put" command, or in the Gaia Portal.</li> <li data-bbox="970 911 1414 1102">f. Start the Check Point services:           <ol style="list-style-type: none"> <li data-bbox="1049 945 1399 1012">i. Connect to the command line.</li> <li data-bbox="1049 1012 1430 1080">ii. Log in to either Gaia Clish, or the Expert mode.</li> <li data-bbox="1049 1080 1287 1125">iii. Run: <code>cpstart</code></li> </ol> </li> </ol>



**Note** - Make sure that there is connectivity between the Security Management Server and the managed Security Gateways in your network.

## 7. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

This step is part of the upgrade procedure of a Security Management Server server. If you upgrade a dedicated Log Server or SmartEvent Server, then skip this step.

If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Security Management Server:

- ["Upgrading a Dedicated Log Server from R80.10 and lower" on page 212](#)
- ["Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228](#)

## 8. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.

Step	Instructions
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 9. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 10. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 11. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Security Management Server from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Security Management Server and the different target Security Management Server.

**Notes:**



- To upgrade from R80.20 and higher, see "["Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration" on page 259](#)".
- These instructions equally apply to:
  - Security Management Server
  - vSEC Controller R80.10 and lower

**Important - Before you upgrade a Security Management Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ").
2	See the " <a href="#">"Upgrade Options and Prerequisites" on page 163</a> ".
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current Security Management Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Security Management Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p> <b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Security Management Server, then export the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the current Security Management Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Security Management Server

Perform a clean install of the R80.40 Security Management Server on another computer.

Do **not** perform initial configuration in SmartConsole.

See "[Installing a Security Management Server](#)" on page 61.



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 Security Management Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Security Management Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre data-bbox="430 406 632 440">cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
4	<p>Transfer the exported databases from an external storage to the R80.40 Security Management Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the files in the binary mode.</p>
5	<p>Make sure the transferred files are not corrupted.</p> <p>Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Security Management Server:</p> <pre data-bbox="430 866 1235 900">md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/bin/upgrade_tools/ directory:</p> <pre data-bbox="430 990 917 1024">cd \$FWDIR/bin/upgrade_tools/</pre>
7	<p>Import the management database:</p> <pre data-bbox="430 1125 1287 1192">yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ If you upgrade from R80 (or higher) version, and the IP addresses of the source and target Security Management Servers <b>are different</b>:       <ol style="list-style-type: none"> <li>a. Issue licenses for the new IP address in your Check Point User Center account.</li> <li>b. Install the new licenses on the R80.40 Security Management Server.</li> </ol> </li> <li>■ If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Security Management Servers <b>must be the same</b>.       <ul style="list-style-type: none"> <li>• If it is necessary to have a different IP address on the R80.40 Security Management Server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.</li> </ul> </li> </ul>

Step	Instructions
8	 <b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower. If <b>SmartEvent</b> Software Blade is enabled on this Security Management Server, then import the <b>Events</b> database. See <a href="#">sk110173</a> .
9	Restart the Check Point services: <pre>cpstop cpstart</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

This step is part of the upgrade procedure of a Security Management Server server. If you upgrade a dedicated Log Server or SmartEvent Server, then skip this step.

If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Security Management Server:

- ["Upgrading a Dedicated Log Server from R80.10 and lower" on page 212](#)
- ["Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228](#)

## 7. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 8. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 9. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 10. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

## 11. Disconnect the old Security Management Server from the network

Disconnect the network cables the old Security Management Server.

## 12. Connect the new Security Management Server to the network

Connect the network cables to the new Security Management Server.

# Upgrading Security Management Servers in Management High Availability from R80.10 and lower

**Notes:**



- To upgrade from R80.20 and higher, see "[Upgrading Security Management Servers in Management High Availability from R80.20 and higher](#)" on page 268.
- These instructions equally apply to:
  - Security Management Servers
  - vSEC Controllers R80.10 and lower

**Important - Before you upgrade a Security Management Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.



**Important - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.**

## Upgrading from R80 or higher versions

Step	Instructions
1	Upgrade the <b>Primary</b> Security Management Server with one of the supported methods. See " <a href="#">Upgrade Methods</a> " on page 175.
2	Upgrade the <b>Secondary</b> Security Management Server with one of the supported methods. See " <a href="#">Upgrade Methods</a> " on page 175.
3	Get the R80.40 SmartConsole. See " <a href="#">Installing SmartConsole</a> " on page 89.
4	Connect with R80.40 SmartConsole to the R80.40 Primary Security Management Server.
5	Update the object version of the Secondary Security Management Server: <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Security Management Server object.</li> <li>From the left tree, click <b>General Properties</b>.</li> <li>In the <b>Platform</b> section &gt; in the <b>Version</b> field, select <b>R80.40</b>.</li> <li>Click <b>OK</b>.</li> </ol>
6	Make sure Secure Internal Communication (SIC) works correctly with the Secondary Security Management Server: <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Security Management Server object.</li> <li>On the <b>General Properties</b> page, click <b>Communication</b>.</li> <li>Click <b>Test SIC Status</b>. The SIC Status must show <b>Communicating</b>.</li> <li>Click <b>Close</b>.</li> <li>Click <b>OK</b>.</li> </ol>
7	Install the management database: <ol style="list-style-type: none"> <li>In the top left corner, click <b>Menu &gt; Install database</b>.</li> <li>Select all objects.</li> <li>Click <b>Install</b>.</li> <li>Click <b>OK</b>.</li> </ol>

Step	Instructions
8	<p>Install the Event Policy.</p> <p> <b>Important</b> - This step applies only if the <b>SmartEvent Correlation Unit Software Blade</b> is enabled on the R80.40 Security Management Server.</p> <ol style="list-style-type: none"> <li>a. In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b>.</li> <li>b. At the top, click <b>+</b> to open a new tab.</li> <li>c. In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b>. The Legacy SmartEvent client opens.</li> <li>d. In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b>.</li> <li>e. Confirm.</li> <li>f. Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded</li> <li>g. Click <b>Close</b>.</li> <li>h. Close the Legacy SmartEvent client.</li> </ol>
9	<p>Reconfigure the Log Exporter:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the server.</li> <li>b. Log in to the Expert mode.</li> <li>c. Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre></li> <li>d. Restart the Log Exporter: <pre>cp_log_export restart</pre></li> </ol> <p>For more information, see the <a href="#">R80.40 Logging and Monitoring Administration Guide</a> &gt; Chapter Log Exporter</p> <p>Synchronize the Security Management Servers:</p> <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Management High Availability</b>.</li> <li>b. In the <b>Peers</b> section, click <b>Actions &gt; Sync Peer</b>.</li> <li>c. The status must show <b>Successfully synced</b> for all peers.</li> </ol>

## Upgrading from R77.30 and lower versions

Step	Instructions
1	Upgrade the <b>Primary</b> Security Management Server with one of the supported methods. See " <a href="#">Upgrade Methods</a> " on page 175.
2	Perform a <i>clean install</i> of the R80.40 on the Secondary Security Management Server. See " <a href="#">Installing a Secondary Security Management Server in Management High Availability</a> " on page 64.
3	Get the R80.40 SmartConsole. See " <a href="#">Installing SmartConsole</a> " on page 89.
4	Connect with R80.40 SmartConsole to the R80.40 Primary Security Management Server.
5	Update the object version of the Secondary Security Management Server: <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Security Management Server object.</li> <li>From the left tree, click <b>General Properties</b>.</li> <li>In the <b>Platform</b> section &gt; in the <b>Version</b> field, select <b>R80.40</b>.</li> <li>Click <b>OK</b>.</li> </ol>
6	Make sure Secure Internal Communication (SIC) works correctly with the Secondary Security Management Server: <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Security Management Server object.</li> <li>On the <b>General Properties</b> page, click <b>Communication</b>.</li> <li>Click <b>Test SIC Status</b>. The SIC Status must show <b>Communicating</b>.</li> <li>Click <b>Close</b>.</li> <li>Click <b>OK</b>.</li> </ol>
7	Install the management database: <ol style="list-style-type: none"> <li>In the top left corner, click <b>Menu &gt; Install database</b>.</li> <li>Select all objects.</li> <li>Click <b>Install</b>.</li> <li>Click <b>OK</b>.</li> </ol>

Step	Instructions
8	<p>Install the Event Policy.</p> <p> <b>Important</b> - This step applies only if the <b>SmartEvent Correlation Unit Software Blade</b> is enabled on the R80.40 Security Management Server.</p> <ol style="list-style-type: none"> <li>a. In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b>.</li> <li>b. At the top, click <b>+</b> to open a new tab.</li> <li>c. In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b>. The Legacy SmartEvent client opens.</li> <li>d. In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b>.</li> <li>e. Confirm.</li> <li>f. Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded</li> <li>g. Click <b>Close</b>.</li> <li>h. Close the Legacy SmartEvent client.</li> </ol>
9	<p>Reconfigure the Log Exporter:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the server.</li> <li>b. Log in to the Expert mode.</li> <li>c. Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre></li> <li>d. Restart the Log Exporter: <pre>cp_log_export restart</pre></li> </ol> <p>For more information, see the <a href="#">R80.40 Logging and Monitoring Administration Guide</a> &gt; Chapter <i>Log Exporter</i></p> <p>Synchronize the Security Management Servers:</p> <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Management High Availability</b>.</li> <li>b. In the <b>Peers</b> section, click <b>Actions &gt; Sync Peer</b>.</li> <li>c. The status must show <b>Successfully synced</b> for all peers.</li> </ol>

# Upgrading a Dedicated Log Server from R80.10 and lower

This section provides instructions to upgrade dedicated Log Servers:

- [\*"Upgrading a Dedicated Log Server from R80.10 and lower with CPUSE" on page 213\*](#)
- [\*"Upgrading a Dedicated Log Server from R80.10 and lower with Advanced Upgrade" on page 216\*](#)
- [\*"Upgrading a Dedicated Log Server from R80.10 and lower with Migration" on page 222\*](#)

# Upgrading a Dedicated Log Server from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same dedicated Log Server or Endpoint Policy Server.

## Notes:



- To upgrade from R80.20 and higher, see "["Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE" on page 245](#)".
- To upgrade a dedicated SmartEvent Server, see "["Upgrading a Dedicated SmartEvent Server from R80.10 and lower with CPUSE" on page 229](#)".
- This upgrade method is supported only for servers that already run on Gaia Operating System.

**Important - Before you upgrade a dedicated Log Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Before you upgrade a dedicated Log Server, you must upgrade the applicable Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the Log Server.

**Procedure:****1. Upgrade the dedicated Log Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**2. Update the version of the Log Server object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated Log Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

**3. Install the management database**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**4. Install the Event Policy on the dedicated Log Server**

**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the dedicated R80.40 Log Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Log Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.

Step	Instructions
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 5. Test the functionality on the dedicated Log Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 Log Server.
2	Make sure the management database and configuration were upgraded correctly.

## 6. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 7. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	Make sure the logging works as expected.

# Upgrading a Dedicated Log Server from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same dedicated Log Server.

## Notes:



- To upgrade from R80.20 and higher, see "[Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade](#)" on page 250.
- To upgrade a dedicated SmartEvent Server, see "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Advanced Upgrade](#)" on page 232.

**Important - Before you upgrade a dedicated Log Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Before you upgrade a dedicated Log Server, you must upgrade the applicable Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the Log Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current dedicated Log Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current dedicated Log Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	<p>Transfer the exported databases from the current server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install the R80.40 Log Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading a Dedicated Log Server from R80.10 and lower" on page 212</a></li> <li>■ <a href="#">"Installing a Dedicated Log Server or SmartEvent Server" on page 67</a></li> </ul>
Operating System other than Gaia	<p>Follow this procedure:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing a Dedicated Log Server or SmartEvent Server" on page 67</a></li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 Log Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Log Server.
2	Log in to the Expert mode.
3	Make sure a valid license is installed: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
4	Transfer the exported databases from an external storage to the R80.40 Log Server, to some directory.  <b>Note</b> - Make sure to transfer the files in the binary mode.
5	Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Log Server: <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	Go to the \$FWDIR/bin/upgrade_tools/ directory: <pre>cd \$FWDIR/bin/upgrade_tools/</pre>
7	Import the management database: <pre>yes   nohup ./migrate import [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre>  <b>Notes:</b> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
8	Restart the Check Point services: <pre>cpstop cpstart</pre>

## 5. Update the version of the Log Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated Log Server.

Step	Instructions
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy on the dedicated Log Server



**Important** - This step applies only if the **SmartEvent Correlation Unit Software Blade** is enabled on the dedicated R80.40 Log Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Log Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the dedicated Log Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 Log Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	Make sure the logging works as expected.

# Upgrading a Dedicated Log Server from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Log Server and the different target Log Server.

**Notes:**



- To upgrade from R80.20 and higher, see "["Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 250.](#)
- To upgrade a dedicated SmartEvent Server, see "["Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Migration" on page 238.](#)

**Important - Before you upgrade a dedicated Log Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">"Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">"Upgrade Options and Prerequisites" on page 163</a> .
3	Before you upgrade a dedicated Log Server, you must upgrade the applicable Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the Log Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current dedicated Log Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current dedicated Log Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	<p>Transfer the exported databases from the current server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Log Server

Perform a clean install of the R80.40 Log Server on another computer.

Do **not** perform initial configuration in SmartConsole.

See "[Installing a Dedicated Log Server or SmartEvent Server](#)" on page 67



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 Log Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Log Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>

Step	Instructions
4	<p>Transfer the exported databases from an external storage to the R80.40 Log Server, to some directory.</p>  <b>Note</b> - Make sure to transfer the files in the binary mode.
5	<p>Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Log Server:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/bin/upgrade_tools/ directory:</p> <pre>cd \$FWDIR/bin/upgrade_tools/</pre>
7	<p>Import the management database:</p> <pre>yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
8	<p>Restart the Check Point services:</p> <pre>cpstop cpstart</pre>

## 5. Update the version of the Log Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated Log Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy on the dedicated Log Server



**Important** - This step applies only if the **SmartEvent Correlation Unit Software Blade** is enabled on the dedicated R80.40 Log Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Log Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the dedicated Log Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 Log Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server.
2	Make sure the logging works as expected.

# Upgrading a Dedicated SmartEvent Server from R80.10 and lower

This section provides instructions to upgrade SmartEvent Servers:

- [\*"Upgrading a Dedicated SmartEvent Server from R80.10 and lower with CPUSE" on page 229\*](#)
- [\*"Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Advanced Upgrade" on page 232\*](#)
- [\*"Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Migration" on page 238\*](#)

# Upgrading a Dedicated SmartEvent Server from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same SmartEvent Server.

## Notes:



- To upgrade from R80.20 and higher, see "[Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE](#)" on page 245.
- To upgrade a dedicated Log Server or Endpoint Policy Server, see "[Upgrading a Dedicated Log Server from R80.10 and lower with CPUSE](#)" on page 213.
- This upgrade method is supported only for servers that already run on Gaia Operating System.

**Important - Before you upgrade a dedicated SmartEvent Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Before you upgrade a dedicated SmartEvent Server, you must upgrade the applicable Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the SmartEvent Server.

**Procedure:****1. Upgrade the dedicated SmartEvent Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**2. Update the version of the SmartEvent Server object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated SmartEvent Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

**3. Install the management database**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**4. Install the Event Policy on the dedicated SmartEvent Server**

**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the dedicated R80.40 SmartEvent Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 SmartEvent Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.

Step	Instructions
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 5. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <code>cp_log_export reconf</code>
4	Restart the Log Exporter: <code>cp_log_export restart</code>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 6. Test the functionality on the dedicated R80.40 SmartEvent Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 SmartEvent Server.
2	Make sure the management database and configuration were upgraded correctly.

## 7. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	Make sure the logging works as expected.

# Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same SmartEvent Server.

## Notes:



- To upgrade from R80.20 and higher, see "[Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade](#)" on page 250.
- To upgrade a dedicated Log Server or Endpoint Policy Server, see "[Upgrading a Dedicated Log Server from R80.10 and lower with Advanced Upgrade](#)" on page 216.
- This upgrade method is supported only for servers that already run on Gaia Operating System.

**Important** - Before you upgrade a dedicated SmartEvent Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Before you upgrade a dedicated SmartEvent Server, you must upgrade the applicable Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the SmartEvent Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current dedicated SmartEvent Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current dedicated SmartEvent Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	<p>Transfer the exported databases from the current server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install the R80.40 SmartEvent Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228</a></li> <li>■ <a href="#">"Installing a Dedicated Log Server or SmartEvent Server" on page 67</a></li> </ul>
Operating System other than Gaia	<p>Follow this procedure:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing a Dedicated Log Server or SmartEvent Server" on page 67</a></li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 SmartEvent Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 SmartEvent Server.
2	Log in to the Expert mode.
3	Make sure a valid license is installed: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
4	Transfer the exported databases from an external storage to the R80.40 SmartEvent Server, to some directory.  <b>Note</b> - Make sure to transfer the files in the binary mode.
5	Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original SmartEvent Server: <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	Go to the \$FWDIR/bin/upgrade_tools/ directory: <pre>cd \$FWDIR/bin/upgrade_tools/</pre>
7	Import the management database: <pre>yes   nohup ./migrate import [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre>  <b>Notes:</b> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
8	Restart the Check Point services: <pre>cpstop cpstart</pre>

## 5. Update the version of the SmartEvent Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated SmartEvent Server.

Step	Instructions
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy on the dedicated SmartEvent Server



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the dedicated R80.40 SmartEvent Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 SmartEvent Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the dedicated R80.40 SmartEvent Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 SmartEvent Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	Make sure the logging works as expected.

# Upgrading a Dedicated SmartEvent Server from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source SmartEvent Server and the different target SmartEvent Server.

## Notes:



- To upgrade from R80.20 and higher, see "["Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration" on page 259](#)".
- To upgrade a dedicated Log Server or Endpoint Policy Server, see "["Upgrading a Dedicated Log Server from R80.10 and lower with Migration" on page 222](#)".
- This upgrade method is supported only for servers that already run on Gaia Operating System.

**Important** - Before you upgrade a dedicated SmartEvent Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Before you upgrade a dedicated SmartEvent Server, you must upgrade the applicable Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the SmartEvent Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current dedicated SmartEvent Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current dedicated SmartEvent Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	<p>Transfer the exported databases from the current server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 SmartEvent Server

Perform a clean install of the R80.40 SmartEvent Server on another computer.

Do **not** perform initial configuration in SmartConsole.

See "[Installing a Dedicated Log Server or SmartEvent Server](#)" on page 67



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 SmartEvent Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 SmartEvent Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>

Step	Instructions
4	<p>Transfer the exported databases from an external storage to the R80.40 SmartEvent Server, to some directory.</p>  <b>Note</b> - Make sure to transfer the files in the binary mode.
5	<p>Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original SmartEvent Server:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/bin/upgrade_tools/ directory:</p> <pre>cd \$FWDIR/bin/upgrade_tools/</pre>
7	<p>Import the management database:</p> <pre>yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
8	<p>Restart the Check Point services:</p> <pre>cpstop cpstart</pre>

## 5. Update the version of the SmartEvent Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated SmartEvent Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy on the dedicated SmartEvent Server



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the dedicated R80.40 SmartEvent Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 SmartEvent Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the dedicated R80.40 SmartEvent Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 SmartEvent Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated SmartEvent Server.
2	Make sure the logging works as expected.

# Upgrading a Security Management Server or Log Server from R80.20 and higher

This section provides instructions to upgrade Security Management Servers and dedicated Log Servers from R80.20.M1, R80.20, R80.20.M2, or R80.30:

- [\*"Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE" on page 245\*](#)
- [\*"Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 250\*](#)
- [\*"Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration" on page 259\*](#)
- [\*"Upgrading Security Management Servers in Management High Availability from R80.20 and higher" on page 268\*](#)

For additional information related to these upgrade procedures, see [sk163814](#).

# Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Check Point server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- These instructions equally apply to:
  - Security Management Server
  - CloudGuard Controller
  - Dedicated Log Server
  - Dedicated SmartEvent Server
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Management Server or Log Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Security Management Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. Upgrade the Security Management Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on [page 160](#) and follow the applicable action plan.

**3. Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on [page 89](#).

**4. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers**

This step is part of the upgrade procedure of a Security Management Server server. If you upgrade a dedicated Log Server or SmartEvent Server, then skip this step."



**Important** - If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Security Management Server.

Select the applicable upgrade option from these:

- For R80.20 and higher:
  - "[Upgrading a Security Management Server or Log Server from R80.20 and higher](#)" on page 244
- For R80.10 and lower:
  - "[Upgrading a Dedicated Log Server from R80.10 and lower](#)" on page 212
  - "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower](#)" on page 228

## 5. Update the object version of the dedicated Log Servers and SmartEvent Servers



**Important** - If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must update the version of the corresponding objects in SmartConsole.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server or SmartEvent Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated Log Server or SmartEvent Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter *Log Exporter*.

## 9. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.

Step	Instructions
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Check Point server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- These instructions equally apply to:
  - Security Management Server
  - CloudGuard Controller
  - Dedicated Log Server
  - Dedicated SmartEvent Server
- For additional information related to this upgrade, see [sk163814](#).

**Important** - Before you upgrade a Management Server or Log Server:



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Security Management Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Security Management Server, run the Pre-Upgrade Verifier and export the**

## entire management database

Step	Instructions
1	Connect to the command line on the source Security Management Server.
2	Log in to the Expert mode.
5	Go to the \$FWDIR/scripts/ directory: <pre>cd \$FWDIR/scripts</pre>
3	Run the Pre-Upgrade Verifier. <ul style="list-style-type: none"> <li>■ If this Security Management Server <i>is</i> connected to the Internet, run:               <pre>./migrate_server verify -v R80.40</pre> </li> <li>■ If this Security Management Server <b>is not</b> connected to the Internet, run:               <pre>./migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> </li> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</p>
4	Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>
4	Export the management database: <ul style="list-style-type: none"> <li>■ If this Security Management Server <i>is</i> connected to the Internet, run:               <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> </li> <li>■ If this Security Management Server <b>is not</b> connected to the Internet, run:               <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> </li> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</p>
7	Calculate the MD5 for the exported database files: <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	Transfer the exported databases from the source Security Management Server to an external storage: <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
	 <b>Note</b> - Make sure to transfer the file in the binary mode.

### 3. Install a new R80.40 Security Management Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Security Management Server only, or Primary Security Management Server in Management High Availability</a>" on page 62.</li> </ul>

**Important** - These options are available:



- The IP addresses of the source and target Security Management Servers **can be the same**.
 

If in the future it is necessary to have a different IP address on the R80.40 Security Management Server, you can change it.  
For applicable procedures, see [sk40993](#) and [sk65451](#).  
Note that you have to issue licenses for the new IP address.
- The IP addresses of the source and target Security Management Servers **can be different**.
 

Note that you have to issue licenses for the new IP address.  
You must install the new licenses only after you import the databases.

#### 4. Get the required Upgrade Tools on the R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a> . (See " <a href="#">Management Server Migration Tool and Upgrade Tools</a> " on page 182.) <b>Note</b> - This is a CPUSE Offline package.
2	Install the R80.40 Upgrade Tools with CPUSE. See " <a href="#">Installing Software Packages on Gaia</a> " on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.

Step	Instructions
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre> <p> <b>Note</b> - The command "migrate_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet. This is to make sure you always have the latest version of these Upgrade Tools installed. If the connection to Check Point Cloud fails, this message appears:</p> <pre>Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.</pre>

## 5. On the target R80.40 Security Management Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Security Management Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre>cplc print</pre> <p>If it is not already installed, then install a valid license now.</p>
4	<p>Transfer the exported databases from an external storage to the R80.40 Security Management Server, to some directory.</p> <p> <b>Note</b> - Make sure to transfer the files in the binary mode.</p>

Step	Instructions
5	<p>Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Security Management Server:</p> <pre data-bbox="441 345 1235 377">md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre data-bbox="441 473 747 505">cd \$FWDIR/scripts/</pre>
7	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Security Management Server <i>is</i> connected to the Internet, run:</li> </ul> <pre data-bbox="525 646 1362 709">./migrate_server import -v R80.40 [-l   -x] &lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Security Management Server is <b>not</b> connected to the Internet, run:</li> </ul> <pre data-bbox="525 781 1399 866">./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] &lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p><b>Important</b> - The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands).</p> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Install the new licenses



**Important** - This step applies only if the target R80.40 Security Management Server has a different IP address than the source Security Management Server.

Step	Instructions
1	Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.
2	Install the new licenses on the R80.40 Security Management Server. You can do this either in the CLI with the "cplic_put" command, or in the Gaia Portal.
3	<p>Wait for a couple of minutes for the Security Management Server to detect the new licenses.</p> <p>Alternatively, restart Check Point services:</p> <pre data-bbox="441 1882 562 1945">cpstop cpstart</pre>

## 8. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

This step is part of the upgrade procedure of a Security Management Server server. If you upgrade a dedicated Log Server or SmartEvent Server, then skip this step."



**Important** - If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Security Management Server.

Select the applicable upgrade option from these:

- For R80.20 and higher:
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For R80.10 and lower:
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 9. Update the object version of the dedicated Log Servers and SmartEvent Servers



**Important** - If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must update the version of the corresponding objects in SmartConsole.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server or SmartEvent Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated Log Server or SmartEvent Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .

Step	Instructions
5	Click <b>OK</b> .

## 11. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 12. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

**13. Test the functionality on the R80.40 Security Management Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration

In a migration and upgrade scenario, you perform the procedure on the source Check Point server and the different target Check Point server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- These instructions equally apply to:
  - Security Management Server
  - Endpoint Security Management Server
  - Dedicated Log Server
  - Dedicated SmartEvent Server
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Management Server or Log Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Security Management Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Security Management Server, run the Pre-Upgrade Verifier and export the**

## entire management database

Step	Instructions
1	Connect to the command line on the source Security Management Server.
2	Log in to the Expert mode.
5	<p>Go to the <code>\$FWDIR/scripts/</code> directory:</p> <pre>cd \$FWDIR/scripts</pre>
3	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Security Management Server <i>is</i> connected to the Internet, run:</li> <pre>./migrate_server verify -v R80.40</pre> <li>■ If this Security Management Server <b>is not</b> connected to the Internet, run:</li> <pre>./migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>
4	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>
4	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Security Management Server <i>is</i> connected to the Internet, run:</li> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <li>■ If this Security Management Server <b>is not</b> connected to the Internet, run:</li> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	<p>Transfer the exported databases from the source Security Management Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
	 <b>Note</b> - Make sure to transfer the file in the binary mode.

### 3. Install a new R80.40 Security Management Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Security Management Server only, or Primary Security Management Server in Management High Availability</a>" on page 62.</li> </ul>

**Important** - These options are available:



- The IP addresses of the source and target Security Management Servers **can be the same**.
 

If in the future it is necessary to have a different IP address on the R80.40 Security Management Server, you can change it.  
For applicable procedures, see [sk40993](#) and [sk65451](#).  
Note that you have to issue licenses for the new IP address.
- The IP addresses of the source and target Security Management Servers **can be different**.
 

Note that you have to issue licenses for the new IP address.  
You must install the new licenses only after you import the databases.

#### 4. Get the required Upgrade Tools on the target R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a> . (See " <a href="#">Management Server Migration Tool and Upgrade Tools</a> " on page 182.) <b>Note</b> - This is a CPUSE Offline package.
2	Install the R80.40 Upgrade Tools with CPUSE. See " <a href="#">Installing Software Packages on Gaia</a> " on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.

Step	Instructions
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre> <p> <b>Note</b> - The command "migrate_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet. This is to make sure you always have the latest version of these Upgrade Tools installed. If the connection to Check Point Cloud fails, this message appears:</p> <pre>Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.</pre>

## 5. On the target R80.40 Security Management Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Security Management Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre>clic print</pre> <p>If it is not already installed, then install a valid license now.</p>
4	<p>Transfer the exported databases from an external storage to the R80.40 Security Management Server, to some directory.</p> <p> <b>Note</b> - Make sure to transfer the files in the binary mode.</p>

Step	Instructions
5	<p>Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Security Management Server:</p> <pre data-bbox="430 350 1235 384">md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre data-bbox="430 473 743 507">cd \$FWDIR/scripts/</pre>
7	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Security Management Server <i>is</i> connected to the Internet, run:</li> </ul> <pre data-bbox="517 642 1367 709">./migrate_server import -v R80.40 [-l   -x] &lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Security Management Server is <b>not</b> connected to the Internet, run:</li> </ul> <pre data-bbox="517 777 1403 878">./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] &lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p><b>Important</b> - The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands).</p> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Install the new licenses



**Important** - This step applies only if the target R80.40 Security Management Server has a different IP address than the source Security Management Server.

Step	Instructions
1	Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.
2	Install the new licenses on the R80.40 Security Management Server. You can do this either in the CLI with the "cplic_put" command, or in the Gaia Portal.
3	<p>Wait for a couple of minutes for the Security Management Server to detect the new licenses.</p> <p>Alternatively, restart Check Point services:</p> <pre data-bbox="430 1877 562 1945">cpstop cpstart</pre>

## 8. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

This step is part of the upgrade procedure of a Security Management Server server. If you upgrade a dedicated Log Server or SmartEvent Server, then skip this step."



**Important** - If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Security Management Server.

Select the applicable upgrade option from these:

- For R80.20 and higher:
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For R80.10 and lower:
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 9. Update the object version of the dedicated Log Servers and SmartEvent Servers



**Important** - If your Security Management Server manages dedicated Log Servers or SmartEvent Servers, you must update the version of the corresponding objects in SmartConsole.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the dedicated Log Server or SmartEvent Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the dedicated Log Server or SmartEvent Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .

Step	Instructions
5	Click <b>OK</b> .

## 11. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 12. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

**13. Test the functionality on the R80.40 Security Management Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

**14. Disconnect the old Security Management Server from the network**

Disconnect the cables from the old Security Management Server.

**15. Connect the new Security Management Server to the network**

Connect the cables to the new Security Management Server.

# Upgrading Security Management Servers in Management High Availability from R80.20 and higher

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- These instructions equally apply to:
  - Security Management Servers
  - CloudGuard Controllers
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Security Management Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Security Management Server is upgraded and runs, before you start the upgrade on other servers.



**Important - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.**

**Procedure:**

Step	Instructions
1	<p>Upgrade the <b>Primary</b> Security Management Server with one of the supported methods.</p> <ul style="list-style-type: none"> <li>■ CPUSE See "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE</a>" on page 245</li> <li>■ Advanced Upgrade See "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade</a>" on page 250</li> <li>■ Migration See "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration</a>" on page 259</li> </ul>
2	<p>Upgrade the <b>Secondary</b> Security Management Server with one of the supported methods.</p> <ul style="list-style-type: none"> <li>■ CPUSE See "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE</a>" on page 245</li> <li>■ Advanced Upgrade See "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade</a>" on page 250</li> <li>■ Migration See "<a href="#">Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration</a>" on page 259</li> </ul>
3	<p>Get the R80.40 SmartConsole. See "<a href="#">Installing SmartConsole</a>" on page 89.</p>
4	<p>Connect with SmartConsole to the R80.40 Primary Security Management Server.</p>
5	<p>Update the object version of the Secondary Security Management Server:</p> <ol style="list-style-type: none"> <li>a. From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>b. Open the Secondary Security Management Server object.</li> <li>c. From the left tree, click <b>General Properties</b>.</li> <li>d. In the <b>Platform</b> section &gt; in the <b>Version</b> field, select <b>R80.40</b>.</li> <li>e. Click <b>OK</b>.</li> </ol>
6	<p>Make sure Secure Internal Communication (SIC) works correctly with the Secondary Security Management Server:</p> <ol style="list-style-type: none"> <li>a. From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>b. Open the Secondary Security Management Server object.</li> <li>c. On the <b>General Properties</b> page, click <b>Communication</b>.</li> <li>d. Click <b>Test SIC Status</b>. The SIC Status must show <b>Communicating</b>.</li> <li>e. Click <b>Close</b>.</li> <li>f. Click <b>OK</b>.</li> </ol>

Step	Instructions
7	<p>Install the management database:</p> <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Install database</b>.</li> <li>b. Select all objects.</li> <li>c. Click <b>Install</b>.</li> <li>d. Click <b>OK</b>.</li> </ol>
8	<p>Install the Event Policy.</p> <p> <b>Important</b> - This step applies only if the <b>SmartEvent Correlation Unit Software Blade</b> is enabled on the R80.40 Security Management Server.</p> <ol style="list-style-type: none"> <li>a. In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b>.</li> <li>b. At the top, click <b>+</b> to open a new tab.</li> <li>c. In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b>.</li> </ol> <p>The Legacy SmartEvent client opens.</p> <ol style="list-style-type: none"> <li>d. In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b>.</li> <li>e. Confirm.</li> <li>f. Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded</li> <li>g. Click <b>Close</b>.</li> <li>h. Close the Legacy SmartEvent client.</li> </ol>
9	<p>Reconfigure the Log Exporter:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the server.</li> <li>b. Log in to the Expert mode.</li> <li>c. Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre></li> <li>d. Restart the Log Exporter: <pre>cp_log_export restart</pre></li> </ol>
10	<p>For more information, see the <a href="#">R80.40 Logging and Monitoring Administration Guide</a> &gt; Chapter <i>Log Exporter</i></p> <p>Synchronize the Security Management Servers:</p> <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Management High Availability</b>.</li> <li>b. In the <b>Peers</b> section, click <b>Actions &gt; Sync Peer</b>.</li> <li>c. The status must show <b>Successfully synced</b> for all peers.</li> </ol>

# Upgrade of Multi-Domain Servers and Multi-Domain Log Servers

This section provides instructions to upgrade Multi-Domain Servers and Multi-Domain Log Servers:

- "[Upgrading one Multi-Domain Server from R80.10 and lower](#)" on page 272
- "[Upgrading one Multi-Domain Server from R80.20 and higher](#)" on page 305
- "[Upgrading Multi-Domain Servers in High Availability from R80.10 and lower](#)" on page 323
- "[Upgrading Multi-Domain Servers in High Availability from R80.20 and higher](#)" on page 358
- "[Upgrading a Multi-Domain Log Server from R80.10 and lower](#)" on page 409
- "[Upgrading a Multi-Domain Log Server from R80.20 and higher](#)" on page 430

# Upgrading one Multi-Domain Server from R80.10 and lower

This section provides instructions to upgrade a Multi-Domain Server from R80.10 and lower:

- [\*"Upgrading one Multi-Domain Server from R80.10 and lower with CPUSE" on page 273\*](#)
- [\*"Upgrading one Multi-Domain Server from R80.10 and lower with Advanced Upgrade" on page 277\*](#)
- [\*"Upgrading one Multi-Domain Server from R80.10 and lower with Migration" on page 285\*](#)
- [\*"Upgrading one R7x Multi-Domain Server with Gradual Migration of Domain Management Servers" on page 293\*](#)



**Important** - You must upgrade the Multi-Domain Server before you can upgrade the Multi-Domain Log Server, dedicated Log Servers, and dedicated SmartEvent Servers.



**Note** - To upgrade from R80.20 and higher, see [\*"Upgrading one Multi-Domain Server from R80.20 and higher" on page 305\*](#).

For configuration information, see the [\*R80.40 Multi-Domain Security Management Administration Guide\*](#).

# Upgrading one Multi-Domain Server from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Server.

## Notes:



- To upgrade from R80.20 and higher, see "[Upgrading one Multi-Domain Server from R80.20 and higher with CPUSE](#)" on page 306.
- This upgrade method is supported only for servers that already run Gaia Operating System.

**Important - Before you upgrade a Multi-Domain Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to each Domain Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	In Multi-Domain Server R80 or R80.10 with enabled vSEC Controller: <ol style="list-style-type: none"> <li>a. Connect with SmartConsole to the Global Domain.</li> <li>b. Delete all global Data Centers objects.</li> <li>c. Assign the modified Global Policies.</li> </ol>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Upgrade the Multi-Domain Server with CPUSE**

See "["Installing Software Packages on Gaia" on page 160](#)" and follow the applicable action plan.

**2. Install the R80.40 SmartConsole**

See "["Installing SmartConsole" on page 89](#)".

**3. Install the management database on each Domain Management Server**

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**4. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers**

**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 430](#)
  - "["Upgrading a Security Management Server or Log Server from R80.20 and higher" on page 244](#)
- For servers R80.10 and lower:
  - "["Upgrading a Multi-Domain Log Server from R80.10 and lower" on page 409](#)
  - "["Upgrading a Dedicated Log Server from R80.10 and lower" on page 212](#)
  - "["Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228](#)

**5. Upgrade the attributes of all managed objects in all Domain Management Servers**

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.

Step	Instructions
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 361 562 393">mdsstat</pre>
	<p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p>
	<pre data-bbox="430 541 1422 595">mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 608 1422 662">mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 676 562 707">mdsstat</pre>
5	Go to the main MDS context:
	<pre data-bbox="430 810 546 842">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p>
	<pre data-bbox="430 968 1251 999">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre>
	<p><b>Notes:</b></p>
	<ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul>
	<pre data-bbox="636 1181 1319 1248">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre>
	<ul style="list-style-type: none"> <li>■ You can perform this action on one Domain Management Server at a time with this command:</li> </ul>
	<pre data-bbox="636 1349 1383 1417">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Management Server&gt;</pre>
7	Allow the database synchronization to run:
	<pre data-bbox="430 1516 1251 1560">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0"</pre> <pre data-bbox="430 1551 1013 1583">AfterUpgradeDbsyncIndication 1 1 0</pre>
	<p>Restart the Check Point services:</p>
	<pre data-bbox="430 1659 546 1691">mdsstop</pre> <pre data-bbox="430 1695 578 1727">mdsstart</pre>
	<p>For more information, see <a href="#">sk121718</a>.</p>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 6. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	<p>Reconfigure the Log Exporter:</p> <pre>cp_log_export reconf</pre>
4	<p>Restart the Log Exporter:</p> <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 7. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading one Multi-Domain Server from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Server.

## Notes:



- To upgrade from R80.20 and higher, see "[Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade](#)" on page 309.
- This upgrade method is supported only for servers that already run Gaia Operating System.

**Important - Before you upgrade a Multi-Domain Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to each Domain Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	In Multi-Domain Server R80 or R80.10 with enabled vSEC Controller: <ol style="list-style-type: none"> <li>a. Connect with SmartConsole to the Global Domain.</li> <li>b. Delete all global Data Centers objects.</li> <li>c. Assign the modified Global Policies.</li> </ol>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the R80.40 installation image**

Step	Instructions
1	Download the R80.40 Clean Install ISO file from the <a href="#">R80.40 Home Page SK</a> .
2	Transfer the R80.40 ISO file to the current server to some directory (for example, /var/log/path_to_iso/).



**Note** - Make sure to transfer the file in the binary mode.

**2. On the current Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services: <pre>mdsstop</pre>
5	Go to the main MDS context: <pre>mdsenv</pre>
6	Mount the R80.40 ISO file: <pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO: <pre>cd /mnt/cdrom/linux/p1_install/</pre>
8	Run the installation script: <pre>./mds_setup</pre> This menu shows: <pre>(1) Run Pre-upgrade verification only [recommended before upgrade] (2) Backup current Multi-Domain Server (3) Export current Multi-Domain Server Or 'Q' to quit.</pre>

Step	Instructions
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services:  <pre>mdsstart</pre> </li> <li>b. Follow the instructions in the report.</li> <li>c. Connect with SmartConsole to the Global Domain that is currently in the Active state.</li> <li>d. Reassign the <b>Global Policy</b> on all Domains.</li> <li>e. In a Management High Availability environment R77.30 and lower:  If you made changes, synchronize the Domain Management Servers immediately after these changes.  (In R80 and higher, this synchronization occurs automatically.)</li> <li>f. Stop all Check Point services again:  <pre>mdsstop</pre> </li> <li>g. Run the installation script again:  <pre>./mds_setup</pre> </li> </ol> <p>This menu shows:</p> <pre>(1) Run Pre-upgrade verification only [recommended before upgrade] (2) Backup current Multi-Domain Server (3) Export current Multi-Domain Server Or 'Q' to quit.</pre>
11	Enter <b>3</b> to export the current Multi-Domain Server configuration.
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): <b>/var/log</b> Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre>  <p><b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.</p>

Step	Instructions
13	Make sure the export file is created in the specified directory: <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
14	Calculate the MD5 for the exported file: <pre>md5sum /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
15	Transfer the exported database from the current Multi-Domain Server to an external storage: <pre>/var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install the R80.40 Multi-Domain Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	Follow one of these procedures: <ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading one Multi-Domain Server from R80.10 and lower with CPUSE" on page 273</a></li> <li>■ <a href="#">"Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 71</a></li> </ul>
Operating System other than Gaia	Follow this procedure: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 71</a></li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See ["Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server" on page 681](#).

### 4. On the R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.

Step	Instructions
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
5	<p>Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.</p> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>
6	<p>Make sure the transferred file is not corrupted.</p> <p>Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server:</p> <pre>md5sum /&lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
7	<p>Import the configuration:</p> <pre>yes   nohup \$MDSDIR/scripts/mds_import.sh /&lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;</pre> <p> <b>Notes:</b></p> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate</i>.</li> </ul>
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Install the management database on each Domain Management Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 8. Upgrade the attributes of all managed objects in all Domain Management Servers

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 316 557 345">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="430 485 1399 541">mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 552 1419 608">mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 619 557 649">mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 743 541 772">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p> <pre data-bbox="430 916 1251 945">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre data-bbox="636 1118 1319 1174">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>■ You can perform this action on one Domain Management Server at a time with this command:</li> </ul> <pre data-bbox="636 1289 1383 1347">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Management Server&gt;</pre>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 1450 1251 1518">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1585 573 1641">mdsstopp mdsstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 9. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	<p>Reconfigure the Log Exporter:</p> <pre>cp_log_export reconf</pre>
4	<p>Restart the Log Exporter:</p> <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 10. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading one Multi-Domain Server from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Multi-Domain Server and the different target Multi-Domain Server.

**Notes:**



- To upgrade from R80.20 and higher, see "["Upgrading one Multi-Domain Server from R80.20 and higher with Migration" on page 316](#)".
- This upgrade method is supported only for servers that already run Gaia Operating System.

**Important - Before you upgrade a Multi-Domain Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to each Domain Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	In Multi-Domain Server R80 or R80.10 with enabled vSEC Controller: <ol style="list-style-type: none"> <li>a. Connect with SmartConsole to the Global Domain.</li> <li>b. Delete all global Data Centers objects.</li> <li>c. Assign the modified Global Policies.</li> </ol>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the R80.40 installation image**

Step	Instructions
1	Download the R80.40 Clean Install ISO file from the <a href="#">R80.40 Home Page SK</a> .
2	Transfer the R80.40 ISO file to the current server to some directory (for example, /var/log/path_to_iso/).



**Note** - Make sure to transfer the file in the binary mode.

**2. On the current Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services: <pre>mdsstop</pre>
5	Go to the main MDS context: <pre>mdsenv</pre>
6	Mount the R80.40 ISO file: <pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO: <pre>cd /mnt/cdrom/linux/p1_install/</pre>
8	Run the installation script: <pre>./mds_setup</pre> This menu shows: <pre>(1) Run Pre-upgrade verification only [recommended before upgrade] (2) Backup current Multi-Domain Server (3) Export current Multi-Domain Server Or 'Q' to quit.</pre>

Step	Instructions
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services: <code>mdsstart</code></li> <li>b. Follow the instructions in the report.</li> <li>c. Connect with SmartConsole to the Global Domain that is currently in the Active state.</li> <li>d. Reassign the <b>Global Policy</b> on all Domains.</li> <li>e. In a Management High Availability environment R77.30 and lower: If you made changes, synchronize the Domain Management Servers immediately after these changes. (In R80 and higher, this synchronization occurs automatically.)</li> <li>f. Stop all Check Point services again: <code>mdsstop</code></li> <li>g. Run the installation script again: <code>./mds_setup</code></li> </ol> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server Or 'Q' to quit.</li> </ul>
11	Enter <b>3</b> to export the current Multi-Domain Server configuration.
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): <b>/var/log</b> Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre>  <p><b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.</p>

Step	Instructions
13	Make sure the export file is created in the specified directory: <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
14	Calculate the MD5 for the exported file: <pre>md5sum /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
15	Transfer the exported database from the current Multi-Domain Server to an external storage: <pre>/var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability</a>" on page 71.</li> </ul>



**Important** - The IP addresses of the source and target server **can be different**. If it is necessary to have a different IP address on the target R80.40 server, **you must create a special JSON configuration file before you import the management database** from the source server. Note that you have to issue licenses for the new IP address. **You must use the same JSON configuration file on all servers in the same Multi-Domain Security Management environment.**

### 4. On the R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
5	<p>Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>
6	<p>Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server:</p> <pre>md5sum &lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
7	<p>Import the configuration:</p> <pre>yes   nohup \$MDSDIR/scripts/mds_import.sh &lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i>.</li> </ul>
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Install the management database on each Domain Management Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server.

Step	Instructions
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "[Upgrading a Multi-Domain Log Server from R80.20 and higher](#)" on page 430
  - "[Upgrading a Security Management Server or Log Server from R80.20 and higher](#)" on page 244
- For servers R80.10 and lower:
  - "[Upgrading a Multi-Domain Log Server from R80.10 and lower](#)" on page 409
  - "[Upgrading a Dedicated Log Server from R80.10 and lower](#)" on page 212
  - "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower](#)" on page 228

## 8. Upgrade the attributes of all managed objects in all Domain Management Servers

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 316 557 345">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="430 473 1399 525">mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 541 1418 615">mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 624 557 653">mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 743 541 772">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p> <pre data-bbox="430 916 1251 945">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre data-bbox="636 1118 1319 1170">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>■ You can perform this action on one Domain Management Server at a time with this command:</li> </ul> <pre data-bbox="636 1282 1383 1334">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Management Server&gt;</pre>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 1450 1251 1525">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1585 573 1648">mdsstopp mdsstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 9. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter:
	<pre>cp_log_export reconf</pre>
4	Restart the Log Exporter:
	<pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 10. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

## 11. Disconnect the old Multi-Domain Server from the network

Disconnect the network cables the old Multi-Domain Server.

## 12. Connect the new Multi-Domain Server to the network

Connect the network cables to the new Multi-Domain Server.

# Upgrading one R7x Multi-Domain Server with Gradual Migration of Domain Management Servers

## Attention:

This upgrade method is supported only when you upgrade from **R7x** versions.

We recommend to upgrade the entire Multi-Domain Server at once with one of these methods:

- "["Upgrading one Multi-Domain Server from R80.10 and lower with CPUSE" on page 273](#)
- "["Upgrading one Multi-Domain Server from R80.10 and lower with Advanced Upgrade" on page 277](#)

Because upgrade of the entire Multi-Domain Server at once is the default recommended method, use the Gradual Migration of Domain Management Servers only in these cases:

- The entire Multi-Domain Server cannot be upgraded at once because of a business impact.
- During the upgrade, it is necessary to rename some or all of the Domain Management Servers.
- In Multi-Domain Server High Availability deployment, it is necessary to change the number of Domain Management Servers on Multi-Domain Servers.

## If you use the Gradual Migration method:

- You must migrate the Global Policies before you migrate the databases from other Domains.
- You can migrate the Global Policies only *one time* from the R7x Multi-Domain Server.
- Until the entire migration procedure is completed, you *cannot* make changes in the Global Policies on the source Multi-Domain Servers.

If it is necessary to make changes on the source Multi-Domain Servers, follow these guidelines:

- If you deleted or modified a global object in the source R7x Multi-Domain Server database, you must make the same changes in the migrated Global Policies on the target R80.40 Multi-Domain Server.
- If you added a global object in the source R7x Multi-Domain Server database, you must delete that global object before you export the databases from other Domains.

**Procedure:****1. Install a new R80.40 Multi-Domain Server**

Perform a clean install of the R80.40 Multi-Domain Server on another computer.

Do **not** perform initial configuration in SmartConsole.

See "[Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability](#)" on page 71.



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "[Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server](#)" on page 681.

**2. Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on page 89.

**3. Create the corresponding Domain Management Servers**

Create the Domain Management Servers, into which you import the entire management database from the source Domain Management Servers.

**Important:**

- Do **not** start the new Domain Management Servers.
- Do **not** configure anything in the new Domain Management Servers.

You can create the Domain Management Servers in one of these ways:

- In SmartConsole.

See the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter *Managing Domains* - Section *Creating a New Domain*.

- With the "mgmt\_cli add domain" command.

See the [Check Point Management API Reference](#) - *mgmt\_cli tool* - Chapter *Multi-Domain* - Section *Domain* - Subsection *add domain*.

**4. Export the global management database from the R7x Global Domain**

Step	Instructions
1	Close all GUI clients (SmartConsole applications) connected to the R7x Multi-Domain Server.
2	Connect to the command line on the R7x Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.

Step	Instructions
5	Go to the directory, where you put the R80.40 Management Server Migration Tool package: <pre>cd /var/log/path_to_migration_tool/</pre>
6	Extract the R80.40 Management Server Migration Tool package: <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
7	Go to the main MDS context: <pre>mdsenv</pre>
8	Export the entire management database: <pre>yes   nohup ./migrate export [-f] [-n] /&lt;Full Path&gt;/R7x_global_policies &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ <b>R7x_global_policies</b> is the name of the export file.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i>.</li> </ul>
9	Calculate the MD5 for the exported database file: <pre>md5sum /&lt;Full Path&gt;/R7x_global_policies.tgz</pre>
10	Transfer the exported database from the R7x Multi-Domain Server to an external storage: <pre>/&lt;Full Path&gt;/R7x_global_policies.tgz</pre>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 5. On the R80.40 Multi-Domain Server, import the R7x global management database to the Global Domain



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.   <b>Note</b> - In Multi-Domain Server High Availability environment, connect to the Primary Multi-Domain Server.

Step	Instructions
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure a valid license is installed:</p> <pre data-bbox="425 406 632 473">mdsenv cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
5	<p>Transfer the exported database from an external storage to the R80.40 <b>Primary</b> Multi-Domain Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>
6	<p>Make sure the transferred file is not corrupted.        Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original R7x Multi-Domain Server:</p> <pre data-bbox="430 900 1165 934">md5sum &lt;Full Path&gt;/R7x_global_policies.tgz</pre>
7	<p>Go to the main MDS context:</p> <pre data-bbox="430 1035 541 1069">mdsenv</pre>
8	<p>Import the global management database:</p> <pre data-bbox="430 1170 1252 1237">migrate_global_policies &lt;Full Path&gt;/R7x_global_policies.tgz</pre>  <p><b>Note</b> - This command stops the Multi-Domain Server.</p>
9	<p>Restart the Check Point services:</p> <pre data-bbox="430 1468 573 1536">mdsstop mdsstart</pre>

Step	Instructions
10	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

6. **On the R7x Multi-Domain Server, export the entire management databases from the applicable source Domain Management Servers one by one**

Step	Instructions
1	Connect to the command line on the R7x Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Go to the directory, where you put the R80.40 Management Server Migration Tool package:
	<pre>cd /var/log/path_to_migration_tool/</pre>
5	Extract the R80.40 Management Server Migration Tool package:
	<pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
6	Go to the context of each applicable Domain Management Server:
	<pre>mdsenv &lt;IP Address or Name of Domain Management Server&gt;</pre>
7	Export the entire management database from each applicable Domain Management Server:
	<pre>yes   nohup ./migrate export [-l   -x] /&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;</pre>
	For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i> .
8	Calculate the MD5 for each exported database file:
	<pre>md5sum /&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz</pre>

Step	Instructions
9	<p>Transfer each exported Domain Management Server database from the current Multi-Domain Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz</pre>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>

#### 7. Transfer the exported R7x Domain Management Server management databases to the R80.40 Multi-Domain Server

Step	Instructions
1	<p>Transfer the exported R7x Domain Management Server management databases from an external storage to the R80.40 Multi-Domain Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>
2	<p>Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the R7x Multi-Domain Server:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz</pre>

#### 8. On the target R80.40 Multi-Domain Server, import the entire management database to the applicable target Domain Management Servers one by one

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Unset the shell idle environment variable:</p> <pre>unset TMOUT</pre>

Step	Instructions
5	<p>Import the R7x Domain Management Server management databases one by one:</p> <pre>cma_migrate /&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz /&lt;Full Path&gt;/&lt;\$FWDIR Directory of the New Domain Management Server&gt;/</pre> <p>Example:</p> <pre>cma_migrate /var/log/orig_R7x_database.tgz /opt/CPmds-R80.40/customers/MyDomain3/CPsuite-R80.40/fw1/</pre> <p> <b>Note</b> - This command updates the database schema before it imports. First, the command runs pre-upgrade verification. If no errors are found, migration continues. If there are errors, you must fix them on the source R7x Domain Management Server according to instructions in the error messages. Then do this procedure again.</p>
6	<p>Start the new Domain Management Server with the imported R7x management database:</p> <pre>mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre>
7	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

9. **On the target R80.40 Multi-Domain Server, upgrade the attributes of all managed objects in each target Domain Management Server**

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 309 562 339">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="430 473 1403 525">mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 541 1422 615">mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 624 562 653">mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 743 541 772">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in each new target Domain Management Server (one at a time):</p> <pre data-bbox="430 911 1403 985">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Management Server&gt;</pre> <p> <b>Note</b> - Because the command prompts you for a 'yes/no' for the Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</p> <pre data-bbox="557 1109 1403 1183">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Management Server&gt;</pre>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 1282 1244 1356">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1417 573 1491">mdsstopp mdsstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 10. Configure the Multi-Domain Server administrators and GUI clients

The gradual upgrade does not keep all data.

You must manually redefine and reassign the Multi-Domain Server administrators and GUI clients to Domains after the gradual upgrade.

Step	Instructions
1	<p>Run the <code>mdsconfig</code> command and configure the options <b>Administrators</b> and <b>GUI clients</b>.</p> <p>See "<a href="#">Post-Installation Configuration</a>" on page 154.</p>
2	<p>See the <a href="#"><i>R80.40 Multi-Domain Security Management Administration Guide</i></a> - Chapter <i>Managing Domains</i> - Section <i>Creating a New Domain</i> - Subsection <i>Assigning Trusted Clients to Domains</i>.</p>

## 11. Reset SIC, create a new ICA, and establish SIC Trust with managed Security Gateways

### Important:



- This step applies only if the target R80.40 Domain Management Server has a different IPv4 address than the source R7x Domain Management Server.
- In a Cluster, you must configure all the Cluster Members in the same way.

When a Management Server and a managed Security Gateway establish SIC Trust, the Security Gateway saves the IP address of the Internal Certificate Authority (ICA) of its Management Server. The Security Gateway uses this IP address for Automatic Certificate Renewal process when the certificate on the Security Gateway expires.

To force the Security Gateway to update the saved IP address of the Management Server's ICA, follow *one* of these procedures:

### Reset and establish SIC Trust again (recommended)

#### Warning:



- In Cluster, this procedure can cause a failover.
- Until Check Point processes restart, traffic does not pass through the Security Gateway (Cluster Member).

For more information, see [sk65764: How to reset SIC](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Start the Check Point Configuration Tool. Run:

```
cpconfig
```

- c. Choose the option **Secure Internal Communication** from the menu - enter 5 press the Enter key.

Follow the instructions on the screen to re-initialize the communication and to enter the Activation Key.

- d. Exit the Check Point Configuration Tool.
- e. Wait for Check Point processes to restart.
- f. Connect with SmartConsole to the Management Server that manages the Security Gateway (Cluster) object.
- g. From the left navigation panel, click **Gateways & Servers**.
- h. Double-click the Security Gateway (Cluster) object.
- i. From the left tree, click **General Properties**.  
In a Cluster object, click **Cluster Members** and edit every Cluster Member object.
- j. Click **Communication**.
- k. Click **Reset**.
- l. Enter the same Activation Key you entered on the Security Gateway (Cluster Member).
- m. Click **Initialize**.
- n. The **Trust State** field must show **Trust established**.
- o. Click **Close**.
- p. Click **OK**.
- q. Publish the SmartConsole session.
- r. Install the Access Control Policy on the Security Gateway (Cluster) object.

### **Manually update the saved ICA IP address on the Security Gateway**

For more information, see [sk103356: How to renew SIC after changing IP Address of Security Management Server](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Log in to the Expert mode.
- c. Back up the current \$CPDIR/registry/HKLM\_registry.data file:

```
cp -v $CPDIR/registry/HKLM_registry.data{,_BKP}
```

- d. Edit the current \$CPDIR/registry/HKLM\_registry.data file:

```
vi $CPDIR/registry/HKLM_registry.data
```

- e. Search for:

```
:ICAip
```

Example of the applicable section:

```
: (SIC
  :ICAdn ("O=R80.40-Manager..ntk6rk")
  :MySICname ("CN=R80.40-MyGW,O=R80.40-Manager..ntk6rk")
  :HasCertificate ("[4]1")
  :CertPath ("/opt/CPshrd-R80.40/conf/sic_cert.p12")
  :ICAip (192.168.41.80)
```

- f. Change the value of the ":ICAip" to the new IP address.

- g. Save the changes in the file and exit the editor.

## 12. Rebuild the status of Global VPN communities after the gradual upgrade

The gradual upgrade does not keep all data.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Go to the main MDS context: <pre>mdsenv</pre>
5	Rebuild the status of Global VPN communities: <pre>fwm mds rebuild_global_communities_status all</pre>

## 13. Configure the VPN keys



**Important** - This step applies if the original R7x Domain Management Server managed VPN gateways.

There can be an issue with the IKE certificates after you migrate the management database, if a VPN tunnel is established between a Check Point Security Gateway and an externally managed, third-party gateway.

The VPN Security Gateway presents its IKE certificate to its peer.

The third-party gateway uses the FQDN of the certificate to retrieve the host name and IP address of the Certificate Authority.

If the IKE certificate was issued by a Check Point Internal CA, then the FQDN contains the host name of the original Management Server.

The peer gateway will fail to contact the original server and will not accept the certificate.

To fix:

- Update the external DNS server to resolve the host name to the IP address of the applicable Domain Management Server.
- Revoke the IKE certificate for the Security Gateway and create a new one.

## 14. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <div style="border: 1px solid black; padding: 2px; display: inline-block;"><code>cp_log_export reconf</code></div>
4	Restart the Log Exporter: <div style="border: 1px solid black; padding: 2px; display: inline-block;"><code>cp_log_export restart</code></div>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter *Log Exporter*.

## 15. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly on each Domain Management Server.

# Upgrading one Multi-Domain Server from R80.20 and higher

This section provides instructions to upgrade Multi-Domain Servers from R80.20.M1, R80.20, R80.20.M2, or R80.30:

- *"Upgrading one Multi-Domain Server from R80.20 and higher with CPUSE" on page 306*
- *"Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade" on page 309*
- *"Upgrading one Multi-Domain Server from R80.20 and higher with Migration" on page 316*

For additional information related to these upgrade procedures, see [sk163814](#).

# Upgrading one Multi-Domain Server from R80.20 and higher with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Server.

**Notes:**



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Multi-Domain Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. Upgrade the Multi-Domain Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on [page 160](#) and follow the applicable action plan.

**3. Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on [page 89](#).

**4. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers**



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 5. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <div style="border: 1px solid black; padding: 2px; display: inline-block;">cp_log_export reconf</div>
4	Restart the Log Exporter: <div style="border: 1px solid black; padding: 2px; display: inline-block;">cp_log_export restart</div>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 6. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Server.

**Notes:**



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Multi-Domain Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire**

## management database

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol>
6	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the source Multi-Domain Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability</a>" on page 71.</li> </ul>



**Important** - The IP addresses of the source and target server **can be different**.

If it is necessary to have a different IP address on the target R80.40 server, **you must create a special JSON configuration file before you import the management database** from the source server. Note that you have to issue licenses for the new IP address. **You must use the same JSON configuration file on all servers in the same Multi-Domain Security Management environment.**

### 4. Get the required Upgrade Tools on the R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a> . (See " <a href="#">Management Server Migration Tool and Upgrade Tools</a> " on page 182.) <b>Note</b> - This is a CPUSE Offline package.
2	Install the R80.40 Upgrade Tools with CPUSE. See " <a href="#">Installing Software Packages on Gaia</a> " on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.
3	Make sure the package is installed. Run this command in the Expert mode: <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. <b>Example</b> Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.

## 5. On the R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.   <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> </div>
7	Go to the \$MDS_FWDIR/scripts/ directory: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cd \$MDS_FWDIR/scripts/</pre> </div>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre data-bbox="504 309 1362 377">./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server is <b>not</b> connected to the Internet, run:</li> </ul> <pre data-bbox="504 444 1399 541">./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="435 743 562 772">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="435 916 1419 1080">mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "[Upgrading a Multi-Domain Log Server from R80.20 and higher](#)" on page 430
  - "[Upgrading a Security Management Server or Log Server from R80.20 and higher](#)" on page 244

- For servers R80.10 and lower:

- "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
- "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
- "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading one Multi-Domain Server from R80.20 and higher with Migration

In a migration and upgrade scenario, you perform the procedure on the source Multi-Domain Server and the different target Multi-Domain Server.

**Notes:**



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Multi-Domain Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "*Management Server Migration Tool and Upgrade Tools*" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>.          (See "<i>Management Server Migration Tool and Upgrade Tools</i>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE.          See "<i>Installing Software Packages on Gaia</i>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.          Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p>

Name of the downloaded package: `ngm_upgrade_wrapper_993000222_1.tgz`

```
[Expert@HostName:0]# cprod_util CPPROD_GetValue
CPupgrade-tools-R80.40 BuildNumber 1
993000222
[Expert@HostName:0]#
```



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire**

## management database

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>
6	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the source Multi-Domain Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability</a>" on page 71.</li> </ul>



**Important** - The IP addresses of the source and target server **can be different**.

If it is necessary to have a different IP address on the target R80.40 server, **you must create a special JSON configuration file before you import the management database** from the source server. Note that you have to issue licenses for the new IP address. **You must use the same JSON configuration file on all servers in the same Multi-Domain Security Management environment.**

### 4. Get the required Upgrade Tools on the R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a> . (See " <a href="#">Management Server Migration Tool and Upgrade Tools</a> " on page 182.) <b>Note</b> - This is a CPUSE Offline package.
2	Install the R80.40 Upgrade Tools with CPUSE. See " <a href="#">Installing Software Packages on Gaia</a> " on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.
3	Make sure the package is installed. Run this command in the Expert mode: <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. <b>Example</b> Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

## 5. On the R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.   <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> </div>
7	Go to the \$MDS_FWDIR/scripts/ directory: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cd \$MDS_FWDIR/scripts/</pre> </div>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre data-bbox="504 309 1362 377">./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server is <b>not</b> connected to the Internet, run:</li> </ul> <pre data-bbox="504 444 1399 541">./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="435 743 562 772">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="435 916 1419 1080">mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "[Upgrading a Multi-Domain Log Server from R80.20 and higher](#)" on page 430
  - "[Upgrading a Security Management Server or Log Server from R80.20 and higher](#)" on page 244

- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [\*R80.40 Logging and Monitoring Administration Guide\*](#) > Chapter *Log Exporter*.

## 9. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Disconnect the old Multi-Domain Server from the network

Disconnect the network cables the old Multi-Domain Server.

## 11. Connect the new Multi-Domain Server to the network

Connect the network cables to the new Multi-Domain Server.

# Upgrading Multi-Domain Servers in High Availability from R80.10 and lower

This section provides instructions to upgrade Multi-Domain Servers in High Availability from R80.10 and lower:

- [\*"Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with CPUSE" on page 324\*](#)
- [\*"Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Advanced Upgrade" on page 329\*](#)
- [\*"Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Migration" on page 343\*](#)
- [\*"Managing Domain Management Servers During the Upgrade Process" on page 408\*](#)

**Important** - During the upgrade of Multi-Domain Servers in Management High Availability to R80.40, it is crucial to import the databases in the specific order:



1. Import the database on the **Primary** Multi-Domain Server.  
If the Primary Multi-Domain Server is not available at this time, you must first promote the Secondary Multi-Domain Server to be the Primary.
2. Import the database on the **Secondary** Multi-Domain Servers.



**Important** - You must upgrade the Multi-Domain Servers before you can upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers.



**Important** - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.



**Note** - To upgrade from R80.20 and higher, see [\*"Upgrading Multi-Domain Servers in High Availability from R80.20 and higher" on page 358.\*](#)

For configuration information, see the [R80.40 Multi-Domain Security Management Administration Guide](#).

# Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Servers.

## Notes:



- **Note** - To upgrade from R80.20 and higher, see "[Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with CPUSE](#)" on page 359.
- This upgrade method is supported only for servers that already run Gaia Operating System.

## Important - Before you upgrade Multi-Domain Servers:



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to each Domain Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	In Multi-Domain Server R80 or R80.10 with enabled vSEC Controller: <ol style="list-style-type: none"> <li>a. Connect with SmartConsole to the Global Domain.</li> <li>b. Delete all global Data Centers objects.</li> <li>c. Assign the modified Global Policies.</li> </ol>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.



**Important** - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.

**Procedure:**

- If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary**

For instructions, see the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter Working with High Availability - Section Failure Recovery - Subsection Promoting the Secondary Multi-Domain Server to Primary.

- Upgrade the Primary Multi-Domain Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

- Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on page 89.

- Update the object version of the Secondary Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Primary Multi-Domain Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Secondary Multi-Domain Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

- Install the management database on each Domain Management Server of the Primary Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the Primary Multi-Domain Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

- Upgrade the Secondary Multi-Domain Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**7. Install the management database on each Domain Management Server of the Secondary Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the <b>Secondary Multi-Domain Server</b> .
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**8. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers**



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

**9. Upgrade the attributes of all managed objects in all Domain Management Servers**



**Important** - Perform this steps on every Multi-Domain Server with **Active** Domain Management Servers.

To determine which Multi-Domain Servers run **Active** Domain Management Servers:

- a. Connect with SmartConsole to a Multi-Domain Server and select the **MDS** context.
- b. From the left navigation panel, click **Multi Domain > Domains**.

The table shows Domains and Multi-Domain Servers:

- Every column shows a Multi-Domain Server.
- **Active** Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.
- **Standby** Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 496 562 525">mdsstat</pre>
	<p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="430 676 1419 848">mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 945 546 974">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p> <pre data-bbox="430 1114 1251 1145">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre>
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:       <pre data-bbox="636 1320 1319 1374">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> </li> <li>■ You can perform this action on one Multi-Domain Server at a time with this command:       <pre data-bbox="636 1491 1387 1545">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Multi-Domain Server&gt;</pre> </li> </ul>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 1653 1251 1715">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1787 578 1841">mdsstopp mdsstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 10. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	<p>Reconfigure the Log Exporter:</p> <pre>cp_log_export reconf</pre>
4	<p>Restart the Log Exporter:</p> <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 11. Test the functionality on the Primary R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the <b>Primary</b> R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.
3	Test the Management High Availability functionality.

# Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Servers.



**Note** - To upgrade from R80.20 and higher, see "[Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade](#)" on page 366.

**Important** - Before you upgrade Multi-Domain Servers:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>Connect with the SmartConsole to each Domain Management Server.</li> <li>From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	In Multi-Domain Server R80 or R80.10 with enabled vSEC Controller: <ol style="list-style-type: none"> <li>Connect with SmartConsole to the Global Domain.</li> <li>Delete all global Data Centers objects.</li> <li>Assign the modified Global Policies.</li> </ol>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.



**Important** - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.

**Procedure:**

- If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary**

For instructions, see the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter Working with High Availability - Section Failure Recovery - Subsection Promoting the Secondary Multi-Domain Server to Primary.

- Get the R80.40 installation image**

Step	Instructions
1	Download the R80.40 Clean Install ISO file from the <a href="#">R80.40 Home Page SK</a> .
2	Transfer the R80.40 ISO file to the current server to some directory (for example, /var/log/path_to_iso/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

- On the Primary Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the Primary Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services:  <pre>mdsstop</pre>
5	Go to the main MDS context:  <pre>mdsenv</pre>
6	Mount the R80.40 ISO file:  <pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO:  <pre>cd /mnt/cdrom/linux/p1_install/</pre>

Step	Instructions
8	<p>Run the installation script:</p> <pre data-bbox="441 271 632 305">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services:</li> </ol> <pre data-bbox="520 911 657 938">mdsstart</pre> <ol style="list-style-type: none"> <li>b. Follow the instructions in the report.</li> <li>c. Connect with SmartConsole to the Global Domain that is currently in the Active state.</li> <li>d. Reassign the <b>Global Policy</b> on all Domains.</li> <li>e. In a Management High Availability environment R77.30 and lower: If you made changes, synchronize the Domain Management Servers immediately after these changes. (In R80 and higher, this synchronization occurs automatically.)</li> <li>f. Stop all Check Point services again:</li> </ol> <pre data-bbox="520 1293 641 1320">mdsstop</pre> <ol style="list-style-type: none"> <li>g. Run the installation script again:</li> </ol> <pre data-bbox="520 1383 711 1410">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
11	<p>Enter <b>3</b> to export the current Multi-Domain Server configuration.</p>

Step	Instructions
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): /var/log Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre> <p> <b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.</p>
13	<p>Make sure the export file is created in the specified directory:</p> <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
14	<p>Rename the exported file:</p> <pre>mv -v /var/log/{,Primary_}exported_mds.&lt;DDMMYYYY- HHMMSS&gt;.tgz</pre>
16	<p>Calculate the MD5 for the exported file:</p> <pre>md5sum /var/log/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
16	<p>Transfer the exported database from the current Multi-Domain Server to an external storage:</p> <pre>/var/log/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

#### 4. Install the Primary R80.40 Multi-Domain Server

See the [R80.40 Release Notes](#) for requirements.

**Important** - Do not perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>■ "<a href="#">Upgrading one Multi-Domain Server from R80.10 and lower with CPUSE</a>" on page 273</li> <li>■ "<a href="#">Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability</a>" on page 71</li> </ul>

Current OS	Available options
Operating System other than Gaia	<p>Follow this procedure:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 71</a></li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See ["Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server" on page 681](#).

## 5. On the Primary R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the Primary R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure a valid license is installed:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> <p>If it is not already installed, then install a valid license now.</p>
5	<p>Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <b>Note</b> - Make sure to transfer the file in the binary mode.     </div>
6	<p>Make sure the transferred file is not corrupted.</p> <p>Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Primary Multi-Domain Server:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum &lt;Full Path&gt;/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> </div>
7	<p>Import the configuration:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>yes   nohup \$MDSDIR/scripts/mds_import.sh &lt;Full Path&gt;/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;</pre> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i>.</li> </ul> </div>



- **yes | nohup ... &** are mandatory parts of the syntax.
- For details, see the [R80.40 CLI Reference Guide](#) - Chapter Multi-Domain Security Management Commands - Section *migrate*.

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. On the Secondary Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire management database

Step	Instructions
1	Connect to the command line on the <b>Secondary</b> Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services:
	<pre>mdsstopp</pre>
5	Go to the main MDS context:
	<pre>mdsenv</pre>
6	Mount the R80.40 ISO file:
	<pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO:
	<pre>cd /mnt/cdrom/linux/p1_install/</pre>

Step	Instructions
8	<p>Run the installation script:</p> <pre data-bbox="441 271 632 305">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services:</li> </ol> <pre data-bbox="520 911 657 938">mdsstart</pre> <ol style="list-style-type: none"> <li>b. Follow the instructions in the report.</li> <li>c. Connect with SmartConsole to the Global Domain that is currently in the Active state.</li> <li>d. Reassign the <b>Global Policy</b> on all Domains.</li> <li>e. In a Management High Availability environment R77.30 and lower: If you made changes, synchronize the Domain Management Servers immediately after these changes. (In R80 and higher, this synchronization occurs automatically.)</li> <li>f. Stop all Check Point services again:</li> </ol> <pre data-bbox="520 1298 641 1325">mdsstop</pre> <ol style="list-style-type: none"> <li>g. Run the installation script again:</li> </ol> <pre data-bbox="520 1388 711 1414">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
11	<p>Enter <b>3</b> to export the current Multi-Domain Server configuration.</p>

Step	Instructions
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): /var/log Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre>  <b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.
13	<p>Make sure the export file is created in the specified directory:</p> <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
14	<p>Rename the exported file:</p> <pre>mv -v /var/log/{,Secondary}exported_mds.&lt;DDMMYYYY- HHMMSS&gt;.tgz</pre>
16	<p>Calculate the MD5 for the exported file:</p> <pre>md5sum /var/log/Secondary_exported_mds.&lt;DDMMYYYY- HHMMSS&gt;.tgz</pre>
16	<p>Transfer the exported database from the current Multi-Domain Server to an external storage:</p> <pre>/var/log/Secondary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>  <b>Note</b> - Make sure to transfer the file in the binary mode.

## 8. Install the Secondary R80.40 Multi-Domain Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Upgrading one Multi-Domain Server from R80.10 and lower with CPUSE" on page 273</a></li> <li>▪ <a href="#">"Installing a Secondary Multi-Domain Server in Management High Availability" on page 72</a></li> </ul>

Current OS	Available options
Operating System other than Gaia	Follow this procedure: <ul style="list-style-type: none"> <li>■ <a href="#"><i>"Installing a Secondary Multi-Domain Server in Management High Availability" on page 72</i></a></li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "[\*Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server" on page 681.\*](#)

## 9. On the Secondary R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

The preliminary steps below apply to a Multi-Site setup, in which some of the Domain Management Servers are **Active** on the **Primary** Multi-Domain Server, and some of the Domain Management Servers are **Active** on the **Secondary** Multi-Domain Servers.



**Note** - The example that follows, assumes that you already upgraded the **Primary** Multi-Domain Server, and upgraded one of the **Secondary** Multi-Domain Servers with **Active** Domain Management Servers on it.

- a. Before you can import the entire management database on the **second** Secondary Multi-Domain Server:
  - a. Connect with SmartConsole to each of the upgraded Multi-Domain Servers:
    - The **Primary** Multi-Domain Server
    - The **first** Secondary Multi-Domain Server
  - b. Make sure the High Availability status of each Multi-Domain Server with the other upgraded Multi-Domain Servers is **OK**.
In case of a failure, you must resolve it **before** you can import the database.
  - c. Import the entire management database on the **second** Secondary Multi-Domain Server.

- b. Before you can import the entire management database on the **third** Secondary Multi-Domain Server:
- Connect with SmartConsole to each of the upgraded Multi-Domain Servers:
    - The Primary Multi-Domain Server
    - The **first** Secondary Multi-Domain Server
    - The **second** Secondary Multi-Domain Server
  - Make sure the High Availability status of each Multi-Domain Server with the other upgraded Multi-Domain Servers is **OK**.  
In case of a failure, you must resolve it **before** you can import the database.
  - Import the entire management database on the **third** Secondary Multi-Domain Server.

Repeat the above test on all other Secondary Multi-Domain Servers before you import the entire management database on them.

Step	Instructions
1	Connect to the command line on the <b>Secondary</b> R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">           cplic print         </div> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.  <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Secondary Multi-Domain Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">           md5sum /&lt;Full Path&gt;/Secondary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz         </div>
7	Import the configuration: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">           yes   nohup \$MDSDIR/scripts/mds_import.sh /&lt;Full Path&gt;/Secondary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;         </div>  <b>Notes:</b> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate</i>.</li> </ul>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

#### 10. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 <b>Primary</b> Multi-Domain Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Secondary Multi-Domain Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

#### 11. Install the management database on each Domain Management Server of the Primary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the <b>Primary</b> Multi-Domain Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

#### 12. Install the management database on each Domain Management Server of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the <b>Secondary</b> Multi-Domain Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

### 13. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

### 14. Upgrade the attributes of all managed objects in all Domain Management Servers



**Important** - Perform this steps on every Multi-Domain Server with **Active** Domain Management Servers.

To determine which Multi-Domain Servers run **Active** Domain Management Servers:

- a. Connect with SmartConsole to a Multi-Domain Server and select the **MDS** context.
- b. From the left navigation panel, click **Multi Domain > Domains**.

The table shows Domains and Multi-Domain Servers:

- Every column shows a Multi-Domain Server.
- **Active** Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.
- **Standby** Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.

Step	Instructions
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 444 562 473">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="430 608 1419 777">mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 878 541 907">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p> <pre data-bbox="430 1046 1251 1075">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:       <pre data-bbox="636 1253 1319 1313">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> </li> <li>■ You can perform this action on one Multi-Domain Server at a time with this command:       <pre data-bbox="636 1417 1383 1477">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Multi-Domain Server&gt;</pre> </li> </ul>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 1585 1251 1646">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1713 573 1774">mdsstopp mdsstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 15. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter:
	<pre>cp_log_export reconf</pre>
4	Restart the Log Exporter:
	<pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 16. Test the functionality on the Primary R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the <b>Primary</b> R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.
3	Test the Management High Availability functionality.

# Upgrading Multi-Domain Servers in High Availability from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Multi-Domain Servers and the different target Multi-Domain Servers.



**Note** - To upgrade from R80.20 and higher, see "[Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration](#)" on page 387.

**Important** - Before you upgrade Multi-Domain Servers:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>Connect with the SmartConsole to each Domain Management Server.</li> <li>From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	In Multi-Domain Server R80 or R80.10 with enabled vSEC Controller: <ol style="list-style-type: none"> <li>Connect with SmartConsole to the Global Domain.</li> <li>Delete all global Data Centers objects.</li> <li>Assign the modified Global Policies.</li> </ol>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.



**Important** - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.

**Procedure:**

- If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary**

For instructions, see the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter Working with High Availability - Section Failure Recovery - Subsection Promoting the Secondary Multi-Domain Server to Primary.

- Get the R80.40 installation image**

Step	Instructions
1	Download the R80.40 Clean Install ISO file from the <a href="#">R80.40 Home Page SK</a> .
2	Transfer the R80.40 ISO file to the current server to some directory (for example, /var/log/path_to_iso/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

- On the Primary Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the Primary Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services:  <pre>mdsstop</pre>
5	Go to the main MDS context:  <pre>mdsenv</pre>
6	Mount the R80.40 ISO file:  <pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO:  <pre>cd /mnt/cdrom/linux/p1_install/</pre>

Step	Instructions
8	<p>Run the installation script:</p> <pre data-bbox="441 271 632 305">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services:</li> </ol> <pre data-bbox="517 911 657 938">mdsstart</pre> <ol style="list-style-type: none"> <li>b. Follow the instructions in the report.</li> <li>c. Connect with SmartConsole to the Global Domain that is currently in the Active state.</li> <li>d. Reassign the <b>Global Policy</b> on all Domains.</li> <li>e. In a Management High Availability environment R77.30 and lower: If you made changes, synchronize the Domain Management Servers immediately after these changes. (In R80 and higher, this synchronization occurs automatically.)</li> <li>f. Stop all Check Point services again:</li> </ol> <pre data-bbox="517 1298 641 1325">mdsstop</pre> <ol style="list-style-type: none"> <li>g. Run the installation script again:</li> </ol> <pre data-bbox="517 1388 711 1414">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
11	<p>Enter <b>3</b> to export the current Multi-Domain Server configuration.</p>

Step	Instructions
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): /var/log Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre> <p> <b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.</p>
13	<p>Make sure the export file is created in the specified directory:</p> <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
14	<p>Rename the exported file:</p> <pre>mv -v /var/log/{,Primary_}exported_mds.&lt;DDMMYYYY- HHMMSS&gt;.tgz</pre>
16	<p>Calculate the MD5 for the exported file:</p> <pre>md5sum /var/log/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
16	<p>Transfer the exported database from the current Multi-Domain Server to an external storage:</p> <pre>/var/log/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

#### 4. Install another Primary R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	<p>Perform the clean install on another server in one of these ways (do <b>not</b> perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability</a>" on page 71.</li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "[Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server](#)" on page 681.

## 5. On the Primary R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the <b>Primary R80.40 Multi-Domain Server</b> .
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.   <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Primary Multi-Domain Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum &lt;Full Path&gt;/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> </div>
7	Import the configuration: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>yes   nohup \$MDSDIR/scripts/mds_import.sh &lt;Full Path&gt;/Primary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;</pre> </div>  <b>Notes:</b> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate</i>.</li> </ul>

Step	Instructions
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. On the Secondary Multi-Domain Server, run the Pre-Upgrade Verifier and export the entire management database

Step	Instructions
1	Connect to the command line on the <b>Secondary</b> Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services:
	<pre>mdsstopp</pre>
5	Go to the main MDS context:
	<pre>mdsenv</pre>
6	Mount the R80.40 ISO file:
	<pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO:
	<pre>cd /mnt/cdrom/linux/p1_install/</pre>

Step	Instructions
8	<p>Run the installation script:</p> <pre data-bbox="441 271 632 305">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services:</li> </ol> <pre data-bbox="517 911 657 938">mdsstart</pre> <ol style="list-style-type: none"> <li>b. Follow the instructions in the report.</li> <li>c. Connect with SmartConsole to the Global Domain that is currently in the Active state.</li> <li>d. Reassign the <b>Global Policy</b> on all Domains.</li> <li>e. In a Management High Availability environment R77.30 and lower: If you made changes, synchronize the Domain Management Servers immediately after these changes. (In R80 and higher, this synchronization occurs automatically.)</li> <li>f. Stop all Check Point services again:</li> </ol> <pre data-bbox="517 1298 641 1325">mdsstop</pre> <ol style="list-style-type: none"> <li>g. Run the installation script again:</li> </ol> <pre data-bbox="517 1388 711 1414">./mds_setup</pre> <p>This menu shows:</p> <ul style="list-style-type: none"> <li>(1) Run Pre-upgrade verification only [recommended before upgrade]</li> <li>(2) Backup current Multi-Domain Server</li> <li>(3) Export current Multi-Domain Server</li> </ul> <p>Or 'Q' to quit.</p>
11	<p>Enter <b>3</b> to export the current Multi-Domain Server configuration.</p>

Step	Instructions
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): /var/log Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre> <p> <b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.</p>
13	<p>Make sure the export file is created in the specified directory:</p> <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
14	<p>Rename the exported file:</p> <pre>mv -v /var/log/{,Secondary}exported_mds.&lt;DDMMYYYY- HHMMSS&gt;.tgz</pre>
16	<p>Calculate the MD5 for the exported file:</p> <pre>md5sum /var/log/Secondary_exported_mds.&lt;DDMMYYYY- HHMMSS&gt;.tgz</pre>
16	<p>Transfer the exported database from the current Multi-Domain Server to an external storage:</p> <pre>/var/log/Secondary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 8. Install another Secondary R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	<p>Perform the clean install on another server in one of these ways (do <b>not</b> perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing a Secondary Multi-Domain Server in Management High Availability</a>" on page 72.</li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "[Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server](#)" on page 681.

## 9. On the Secondary R80.40 Multi-Domain Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

The preliminary steps below apply to a Multi-Site setup, in which some of the Domain Management Servers are **Active** on the **Primary** Multi-Domain Server, and some of the Domain Management Servers are **Active** on the **Secondary** Multi-Domain Servers.



**Note** - The example that follows, assumes that you already upgraded the **Primary** Multi-Domain Server, and upgraded one of the **Secondary** Multi-Domain Servers with **Active** Domain Management Servers on it.

- a. Before you can import the entire management database on the **second** Secondary Multi-Domain Server:
  - a. Connect with SmartConsole to each of the upgraded Multi-Domain Servers:
    - The **Primary** Multi-Domain Server
    - The **first** Secondary Multi-Domain Server
  - b. Make sure the High Availability status of each Multi-Domain Server with the other upgraded Multi-Domain Servers is **OK**.
 

In case of a failure, you must resolve it **before** you can import the database.
  - c. Import the entire management database on the **second** Secondary Multi-Domain Server.
- b. Before you can import the entire management database on the **third** Secondary Multi-Domain Server:
  - a. Connect with SmartConsole to each of the upgraded Multi-Domain Servers:
    - The **Primary** Multi-Domain Server
    - The **first** Secondary Multi-Domain Server
    - The **second** Secondary Multi-Domain Server
  - b. Make sure the High Availability status of each Multi-Domain Server with the other upgraded Multi-Domain Servers is **OK**.
 

In case of a failure, you must resolve it **before** you can import the database.
  - c. Import the entire management database on the **third** Secondary Multi-Domain Server.

Repeat the above test on all other Secondary Multi-Domain Servers before you import the entire management database on them.

Step	Instructions
1	Connect to the command line on the <b>Secondary</b> R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div>
	If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.
	 <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Secondary Multi-Domain Server:
	<div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum &lt;Full Path&gt;/Secondary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre> </div>
7	Import the configuration:
	<div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>yes   nohup \$MDSDIR/scripts/mds_import.sh &lt;Full Path&gt;/Secondary_exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;</pre> </div>
	 <b>Notes:</b> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i>.</li> </ul>
8	Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):
	<div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>mdsstat</pre> </div>
	If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:
	<div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre> </div>

## 10. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Primary Multi-Domain Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Secondary Multi-Domain Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

**11. Install the management database on each Domain Management Server of the Primary Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the Primary Multi-Domain Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**12. Install the management database on each Domain Management Server of the Secondary Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the Secondary Multi-Domain Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**13. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers**



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

#### 14. Upgrade the attributes of all managed objects in all Domain Management Servers



**Important** - Perform this steps on every Multi-Domain Server with **Active** Domain Management Servers.

To determine which Multi-Domain Servers run **Active** Domain Management Servers:

- a. Connect with SmartConsole to a Multi-Domain Server and select the **MDS** context.
- b. From the left navigation panel, click **Multi Domain > Domains**.

The table shows Domains and Multi-Domain Servers:

- Every column shows a Multi-Domain Server.
- **Active** Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.
- **Standby** Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable): <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>mdsstat</pre> </div> If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre> </div>

Step	Instructions
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 271 541 300">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p> <pre data-bbox="430 440 1251 471">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre data-bbox="636 642 1314 698">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>■ You can perform this action on one Multi-Domain Server at a time with this command:</li> </ul> <pre data-bbox="636 810 1383 866">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Multi-Domain Server&gt;</pre>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 979 1251 1035">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1114 573 1170">mdsstop mdsstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>
8	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 1338 557 1367">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre data-bbox="430 1518 1414 1686">mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 15. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 16. Test the functionality on the Primary R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the <b>Primary</b> R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.
3	Test the Management High Availability functionality.

## 17. Disconnect the old Multi-Domain Servers from the network

Disconnect the network cables the old Multi-Domain Servers.

## 18. Connect the new Multi-Domain Servers to the network

Connect the network cables to the new Multi-Domain Servers.

# Managing Domain Management Servers During the Upgrade Process



**Best Practice** - To not make any changes to Domain Management Server databases during the upgrade process.

If your business model cannot support management downtime during the upgrade, you can continue to manage Domain Management Servers during the upgrade process.

If you make changes to Domain Management Server databases during the upgrade process, this can create a risk of inconsistent Domain Management Server database content between instances on different Multi-Domain Servers. The synchronization process cannot resolve these database inconsistencies.

After you successfully upgrade one Multi-Domain Server, you can set its Domain Management Servers to the **Active** state, while you upgrade the others. Synchronization between the Domain Management Servers occurs after all Multi-Domain Servers are upgraded.

If, during the upgrade process, you make changes to the Domain Management Server database on different Multi-Domain Servers, the contents of these databases will be different. Because you cannot synchronize these databases, some of these changes will be lost. The Domain Management Server High Availability status appears as **Collision**.

You must decide which database version to retain and synchronize it to the other Domain Management Servers. Then you must re-enter the lost changes to the synchronized database - configure the same objects and settings again.

# Upgrading Multi-Domain Servers in High Availability from R80.20 and higher

This section provides instructions to upgrade Multi-Domain Servers in High Availability from R80.20.M1, R80.20, R80.20.M2, or R80.30:

- [\*"Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with CPUSE" on page 359\*](#)
- [\*"Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade" on page 366\*](#)
- [\*"Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration" on page 387\*](#)
- [\*"Managing Domain Management Servers During the Upgrade Process" on page 408\*](#)

For additional information related to these upgrade procedures, see [sk163814](#).

For configuration information, see the [\*R80.40 Multi-Domain Security Management Administration Guide\*](#).



**Important** - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.

# Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Servers.

**Notes:**



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade Multi-Domain Servers:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.



**Important - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.**

**Procedure:**

- If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary**

For instructions, see the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter Working with High Availability - Section Failure Recovery - Subsection Promoting the Secondary Multi-Domain Server to Primary.

- Get the required Upgrade Tools on the Primary Multi-Domain Server**



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

- Upgrade the Primary Multi-Domain Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

- Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on page 89.

## 5. Get the required Upgrade Tools on the Secondary Multi-Domain Server



**Note** - This step is needed only to be able to export the entire management database (for backup purposes) with the latest Upgrade Tools.



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

## 6. Upgrade the Secondary Multi-Domain Server with CPUSE

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.



**Important** - If you upgrade from R80.20.M1, then you must perform a clean install of the Secondary R80.40 Multi-Domain Server:

- a. See the [R80.40 Release Notes](#) for requirements.
- b. Follow "*Installing a Secondary Multi-Domain Server in Management High Availability*" on page 72.

Do not perform initial configuration in SmartConsole.

The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "*Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server*" on page 681.

## 7. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Primary Multi-Domain Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Secondary Multi-Domain Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 8. Install the management database on each Domain Management Server of the Primary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the Primary Multi-Domain Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 9. Install the management database on each Domain Management Server of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server of the Secondary Multi-Domain Server.

Step	Instructions
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 10. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 11. Upgrade the attributes of all managed objects in all Domain Management Servers



**Important** - Perform this steps on every Multi-Domain Server with **Active** Domain Management Servers.

To determine which Multi-Domain Servers run **Active** Domain Management Servers:

- a. Connect with SmartConsole to a Multi-Domain Server and select the **MDS** context.
- b. From the left navigation panel, click **Multi Domain > Domains**.

The table shows Domains and Multi-Domain Servers:

- Every column shows a Multi-Domain Server.
- **Active** Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.
- **Standby** Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.

Step	Instructions
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="430 361 562 393">mdsstat</pre>
	<p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p>
	<pre data-bbox="430 532 1422 595">mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 601 1422 664">mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 676 562 707">mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 810 546 842">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p>
	<pre data-bbox="430 968 1251 999">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre>
	<p><b>Notes:</b></p>
	<ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul>
	<pre data-bbox="636 1183 1319 1246">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre>
	<ul style="list-style-type: none"> <li>■ You can perform this action on one Multi-Domain Server at a time with this command:</li> </ul>
	<pre data-bbox="636 1347 1387 1410">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Multi-Domain Server&gt;</pre>
7	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p>
	<pre data-bbox="430 1545 562 1576">mdsstat</pre>
	<p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p>
	<pre data-bbox="430 1715 1422 1778">mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 1785 1422 1848">mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre> <pre data-bbox="430 1859 562 1891">mdsstat</pre>

## 12. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 13. Test the functionality on the Primary R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the <b>Primary</b> R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.
3	Test the Management High Availability functionality.

# Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Servers.

**Notes:**



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade Multi-Domain Servers:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.



**Important - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.**

**Procedure:**

- If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary**

For instructions, see the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter Working with High Availability - Section Failure Recovery - Subsection Promoting the Secondary Multi-Domain Server to Primary.

- Make sure the Global Domain is Active on the Primary Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to the <b>Primary Multi-Domain Server</b> .
2	From the left navigation panel, click <b>Multi Domain &gt; Domains</b> . The table shows Domains and Multi-Domain Servers: <ul style="list-style-type: none"> <li>■ Every column shows a Multi-Domain Server.</li> <li>■ <b>Active</b> Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.</li> <li>■ <b>Standby</b> Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.</li> </ul>
3	In the leftmost column <b>Domains</b> , examine the bottom row <b>Global</b> for the <b>Primary Multi-Domain Server</b> . If the Global Domain is in the <b>Standby</b> state on the <b>Primary Multi-Domain Server</b> (marked with an empty "barrel" icon), then make it <b>Active</b> : <ol style="list-style-type: none"> <li>Right-click on the Primary Multi-Domain Server and click <b>Connect to Domain Server</b>. The <b>High Availability Status</b> window opens.</li> <li>In the section <b>Connected To</b>, click <b>Actions &gt; Set Active</b>.</li> <li>Click <b>Yes</b> to confirm.</li> <li>Wait for the full synchronization to complete.</li> <li>Close SmartConsole.</li> </ol>

- Get the required Upgrade Tools on the Primary and on the Secondary Multi-Domain**

## Servers



**Important** - See "*Management Server Migration Tool and Upgrade Tools*" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>.          (See "<i>Management Server Migration Tool and Upgrade Tools</i>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE.          See "<i>Installing Software Packages on Gaia</i>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.          Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p>

Name of the downloaded package: `ngm_upgrade_wrapper_993000222_1.tgz`

```
[Expert@HostName:0]# cprod_util CPPROD_GetValue
CPupgrade-tools-R80.40 BuildNumber 1
993000222
[Expert@HostName:0]#
```



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

### 4. On the Primary Multi-Domain Server, run the Pre-Upgrade Verifier

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>

## 5. On the Secondary Multi-Domain Server, run the Pre-Upgrade Verifier

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>

## 6. On the Primary Multi-Domain Server, export the entire management database

Step	Instructions
1	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>

Step	Instructions
2	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
3	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/Primary_&lt;Name of Database File&gt;.tgz</pre>
4	<p>Transfer the exported databases from the source Multi-Domain Server to an external storage:</p> <pre>/&lt;Full Path&gt;/Primary_&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 7. On the Secondary Multi-Domain Server, export the entire management database

Step	Instructions
1	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>
2	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
3	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/Secondary_&lt;Name of Database File&gt;.tgz</pre>

Step	Instructions
4	<p>Transfer the exported databases from the source Multi-Domain Server to an external storage:</p> <pre style="border: 1px solid black; padding: 5px; margin-left: 20px;">/&lt;Full Path&gt;/Secondary_&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 8. Install the Primary R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	<ul style="list-style-type: none"> <li>■ If you upgrade from R80.20, R80.20.M2, and higher versions, you can follow one of these procedures:           <ul style="list-style-type: none"> <li>• <a href="#">"Installing Software Packages on Gaia" on page 160</a>. Select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>• <a href="#">"Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 71</a>. Do not perform initial configuration in SmartConsole.</li> </ul> </li> <li>■ If you upgrade from R80.20.M1 version, you must follow this procedure:           <ul style="list-style-type: none"> <li>• <a href="#">"Installing a Secondary Multi-Domain Server in Management High Availability" on page 72</a>. Do not perform initial configuration in SmartConsole.</li> </ul> </li> </ul>



**Important** - The IP addresses of the source and target server **can be different**. If it is necessary to have a different IP address on the target R80.40 server, **you must create a special JSON configuration file before you import the management database** from the source server.

Note that you have to issue licenses for the new IP address.

You must use the same JSON configuration file on all servers in the same Multi-Domain Security Management environment.

## 9. Get the required Upgrade Tools on the Primary server



**Important** - See ["Management Server Migration Tool and Upgrade Tools" on page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See <a href="#">"Management Server Migration Tool and Upgrade Tools" on page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See <a href="#">"Installing Software Packages on Gaia" on page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>

Step	Instructions
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre> <p><b>Note</b> - The command "migrate_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet. This is to make sure you always have the latest version of these Upgrade Tools installed. If the connection to Check Point Cloud fails, this message appears:</p> <pre>Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.</pre>

## 10. On the Primary R80.40 Multi-Domain Server, import the databases

### Required JSON configuration file

If you installed the target R80.40 Multi-Domain Server with a different IP address than the source Multi-Domain Server, **you must create a special JSON configuration file before you import the management database** from the source Multi-Domain Server. Note that you have to issue licenses for the new IP address.

#### Important:



- If none of the servers in the same Multi-Domain Security Management environment changed their original IP addresses, then you do **not** need to create the special JSON configuration file.
- Even if only one of the servers migrates to a new IP address, all the other servers (including all Log Servers and SmartEvent Servers) must get this configuration file for the import process.  
**You must use the same JSON configuration file on all servers (including Log Servers and SmartEvent Servers) in the same Multi-Domain Security Management environment.**

To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R80.40 Multi-Domain Server.

Step	Instructions
2	<p>Log in to the Expert mode.</p>
3	<p>Create the <code>/var/log/mdss.json</code> file that contains <b>each</b> server migrated to a new IP address.</p> <p><b>Format for migrating only the Primary Multi-Domain Server to a new IP address</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;" }]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;"}]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Multi-Domain Log Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of R80.40 Multi-Domain Log Server&gt;"}]</pre>

Step	Instructions
	<p><b>Example</b></p> <p>There are 3 servers in the R80.30 Multi-Domain Security Management environment - the Primary Multi-Domain Server, the Secondary Multi-Domain Server, and the Multi-Domain Log Server. Both the Primary and the Secondary Multi-Domain Servers are migrated to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> <li>The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21</li> <li>The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22</li> <li>The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS</li> <li>The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS</li> <li>The new IPv4 address of the target Primary R80.40 Multi-Domain Server is: 172.30.40.51</li> <li>The new IPv4 address of the target Secondary R80.40 Multi-Domain Server is: 172.30.40.52</li> <li>The required syntax for the JSON configuration file you must use on both the Primary and the Secondary Multi-Domain Servers, and on the Multi-Domain Log Server:  <pre>[ {"name": "MyPrimaryMDS", "newIpAddress4": "172.30.40.51"}, {"name": "MySecondaryMDS", "newIpAddress4": "172.30.40.52"} ]</pre> </li> </ol> <p> <b>Important</b> - All servers in this environment must get this same information.</p>

## Importing the databases

### Important:



- Make sure you followed the instructions in the above section **"Required JSON configuration file"**.
- Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line the <b>Primary</b> R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed:
	<code>cplic print</code>
	If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.
	 <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server:
	<code>md5sum /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</code>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory:
	<code>cd \$MDS_FWDIR/scripts/</code>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> <li>■ If this Multi-Domain Server is <b>not</b> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 -skip_ upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - skip_upgrade_tools_check -change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 11. Install the Secondary R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.

Step	Instructions
2	<ul style="list-style-type: none"> <li>■ If you upgrade from R80.20, R80.20.M2, and higher versions, you can follow one of these procedures:           <ul style="list-style-type: none"> <li>• "<i>Installing Software Packages on Gaia</i>" on page 160. Select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>• "<i>Installing a Secondary Multi-Domain Server in Management High Availability</i>" on page 72. <b>Do not</b> perform initial configuration in SmartConsole.</li> </ul> </li> <li>■ If you upgrade from R80.20.M1 version, you must follow this procedure:           <ul style="list-style-type: none"> <li>• "<i>Installing a Secondary Multi-Domain Server in Management High Availability</i>" on page 72. <b>Do not</b> perform initial configuration in SmartConsole.</li> </ul> </li> </ul>



**Important** - The IP addresses of the source and target server **can be different**. If it is necessary to have a different IP address on the target R80.40 server, **you must create a special JSON configuration file before you import the management database** from the source server. Note that you have to issue licenses for the new IP address. **You must use the same JSON configuration file on all servers in the same Multi-Domain Security Management environment.**

## 12. Get the required Upgrade Tools on the Secondary R80.40 Multi-Domain Server



**Note** - This step is needed only to be able to export the entire management database (for backup purposes) with the latest Upgrade Tools.



**Important** - See "*Management Server Migration Tool and Upgrade Tools*" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<i>Management Server Migration Tool and Upgrade Tools</i>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<i>Installing Software Packages on Gaia</i>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>

Step	Instructions
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre> <p> <b>Note</b> - The command "migrate_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet. This is to make sure you always have the latest version of these Upgrade Tools installed. If the connection to Check Point Cloud fails, this message appears:</p> <pre>Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.</pre>

### 13. On the Secondary R80.40 Multi-Domain Server, import the databases

#### Required JSON configuration file

If you installed the target R80.40 Multi-Domain Server with a different IP address than the source Multi-Domain Server, **you must create a special JSON configuration file before you import the management database** from the source Multi-Domain Server. Note that you have to issue licenses for the new IP address.

**Important:**



- If none of the servers in the same Multi-Domain Security Management environment changed their original IP addresses, then you do **not** need to create the special JSON configuration file.
- Even if only one of the servers migrates to a new IP address, all the other servers (including all Log Servers and SmartEvent Servers) must get this configuration file for the import process.  
**You must use the same JSON configuration file on all servers (including Log Servers and SmartEvent Servers) in the same Multi-Domain Security Management environment.**

To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R80.40 Multi-Domain Server.

Step	Instructions
2	<p>Log in to the Expert mode.</p>
3	<p>Create the <code>/var/log/mdss.json</code> file that contains <b>each</b> server migrated to a new IP address.</p> <p><b>Format for migrating only the Primary Multi-Domain Server to a new IP address</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;" }]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;"}]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Multi-Domain Log Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of R80.40 Multi-Domain Log Server&gt;"}]</pre>

Step	Instructions
	<p><b>Example</b></p> <p>There are 3 servers in the R80.30 Multi-Domain Security Management environment - the Primary Multi-Domain Server, the Secondary Multi-Domain Server, and the Multi-Domain Log Server. Both the Primary and the Secondary Multi-Domain Servers are migrated to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> <li>a. The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21</li> <li>b. The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22</li> <li>c. The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS</li> <li>d. The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS</li> <li>e. The new IPv4 address of the target Primary R80.40 Multi-Domain Server is: 172.30.40.51</li> <li>f. The new IPv4 address of the target Secondary R80.40 Multi-Domain Server is: 172.30.40.52</li> <li>g. The required syntax for the JSON configuration file you must use on both the Primary and the Secondary Multi-Domain Servers, and on the Multi-Domain Log Server:  <pre>[ {"name": "MyPrimaryMDS", "newIpAddress4": "172.30.40.51"}, {"name": "MySecondaryMDS", "newIpAddress4": "172.30.40.52"} ]</pre> </li> </ol> <p> <b>Important</b> - All servers in this environment must get this same information.</p>

## Importing the databases

### Important:



- Make sure you followed the instructions in the above section **"Required JSON configuration file"**.
- Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line the <b>Secondary R80.40 Multi-Domain Server</b> .
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed:
	<code>cplic print</code>
	If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.
	 <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server:
	<code>md5sum /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</code>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory:
	<code>cd \$MDS_FWDIR/scripts/</code>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> <li>■ If this Multi-Domain Server is <b>not</b> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 -skip_ upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - skip_upgrade_tools_check -change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

#### 14. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

#### 15. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Primary Multi-Domain Server.

Step	Instructions
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Secondary Multi-Domain Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 16. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 17. Install the management database on each Domain Management Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 18. Upgrade the attributes of all managed objects in all Domain Management Servers



**Important** - Perform this steps on every Multi-Domain Server with **Active** Domain Management Servers.  
To determine which Multi-Domain Servers run **Active** Domain Management Servers:

- a. Connect with SmartConsole to a Multi-Domain Server and select the **MDS** context.
- b. From the left navigation panel, click **Multi Domain > Domains**.

The table shows Domains and Multi-Domain Servers:

- Every column shows a Multi-Domain Server.
- **Active** Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.
- **Standby** Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre>mdsenv</pre>

Step	Instructions
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre>yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>You can perform this action on one Multi-Domain Server at a time with this command:</li> </ul> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Multi-Domain Server&gt;</pre>
7	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 19. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter:
	<pre>cp_log_export reconf</pre>
4	Restart the Log Exporter:
	<pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 20. Test the functionality on the Primary R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the <b>Primary</b> R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.
3	Test the Management High Availability functionality.

# Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration

In a migration and upgrade scenario, you perform the procedure on the source Multi-Domain Servers and the different target Multi-Domain Servers.

**Notes:**



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade Multi-Domain Servers:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Multi-Domain Server is upgraded and runs, before you start the upgrade on other servers.



**Important - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.**

**Procedure:**

- If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary**

For instructions, see the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter Working with High Availability - Section Failure Recovery - Subsection Promoting the Secondary Multi-Domain Server to Primary.

- Make sure the Global Domain is Active on the Primary Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to the <b>Primary Multi-Domain Server</b> .
2	From the left navigation panel, click <b>Multi Domain &gt; Domains</b> . The table shows Domains and Multi-Domain Servers: <ul style="list-style-type: none"> <li>■ Every column shows a Multi-Domain Server.</li> <li>■ <b>Active</b> Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.</li> <li>■ <b>Standby</b> Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.</li> </ul>
3	In the leftmost column <b>Domains</b> , examine the bottom row <b>Global</b> for the <b>Primary Multi-Domain Server</b> . If the Global Domain is in the <b>Standby</b> state on the <b>Primary Multi-Domain Server</b> (marked with an empty "barrel" icon), then make it <b>Active</b> : <ol style="list-style-type: none"> <li>Right-click on the Primary Multi-Domain Server and click <b>Connect to Domain Server</b>. The <b>High Availability Status</b> window opens.</li> <li>In the section <b>Connected To</b>, click <b>Actions &gt; Set Active</b>.</li> <li>Click <b>Yes</b> to confirm.</li> <li>Wait for the full synchronization to complete.</li> <li>Close SmartConsole.</li> </ol>

- Get the required Upgrade Tools on the Primary and on the Secondary Multi-Domain**

## Servers



**Important** - See "*Management Server Migration Tool and Upgrade Tools*" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>.          (See "<i>Management Server Migration Tool and Upgrade Tools</i>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE.          See "<i>Installing Software Packages on Gaia</i>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.          Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p>

Name of the downloaded package: `ngm_upgrade_wrapper_993000222_1.tgz`

```
[Expert@HostName:0]# cprod_util CPPROD_GetValue
CPupgrade-tools-R80.40 BuildNumber 1
993000222
[Expert@HostName:0]#
```



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

### 4. On the Primary Multi-Domain Server, run the Pre-Upgrade Verifier

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>

## 5. On the Secondary Multi-Domain Server, run the Pre-Upgrade Verifier

Step	Instructions
1	Connect to the command line on the current Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>

## 6. On the Primary Multi-Domain Server, export the entire management database

Step	Instructions
1	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>

Step	Instructions
2	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
3	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/Primary_&lt;Name of Database File&gt;.tgz</pre>
4	<p>Transfer the exported databases from the source Multi-Domain Server to an external storage:</p> <pre>/&lt;Full Path&gt;/Primary_&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 7. On the Secondary Multi-Domain Server, export the entire management database

Step	Instructions
1	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>
2	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
3	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/Secondary_&lt;Name of Database File&gt;.tgz</pre>

Step	Instructions
4	<p>Transfer the exported databases from the source Multi-Domain Server to an external storage:</p> <pre>/&lt;Full Path&gt;/Secondary_&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 8. Install another Primary R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	<p>Perform the clean install on another server in one of these ways:</p> <p><b>Important</b> - Do not perform initial configuration in SmartConsole.</p> <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160. Select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability</a>" on page 71.</li> </ul>



**Important** - The IP addresses of the source and target server can be different.

If it is necessary to have a different IP address on the target R80.40 server, you must create a special JSON configuration file before you import the management database from the source server.

Note that you have to issue licenses for the new IP address.

You must use the same JSON configuration file on all servers (including Log Servers and SmartEvent Servers) in the same Multi-Domain Security Management environment.

## 9. Get the required Upgrade Tools on the Primary server



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>

Step	Instructions
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre> <p> <b>Note</b> - The command "migrate_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet. This is to make sure you always have the latest version of these Upgrade Tools installed. If the connection to Check Point Cloud fails, this message appears:</p> <pre>Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.</pre>

## 10. On the Primary R80.40 Multi-Domain Server, import the databases

### Required JSON configuration file

If you installed the target R80.40 Multi-Domain Server with a different IP address than the source Multi-Domain Server, **you must create a special JSON configuration file before you import the management database** from the source Multi-Domain Server. Note that you have to issue licenses for the new IP address.

**Important:**



- If none of the servers in the same Multi-Domain Security Management environment changed their original IP addresses, then you do **not** need to create the special JSON configuration file.
- Even if only one of the servers migrates to a new IP address, all the other servers (including all Log Servers and SmartEvent Servers) must get this configuration file for the import process.  
**You must use the same JSON configuration file on all servers (including Log Servers and SmartEvent Servers) in the same Multi-Domain Security Management environment.**

To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R80.40 Multi-Domain Server.

Step	Instructions
2	<p>Log in to the Expert mode.</p>
3	<p>Create the <code>/var/log/mdss.json</code> file that contains <b>each</b> server migrated to a new IP address.</p> <p><b>Format for migrating only the Primary Multi-Domain Server to a new IP address</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;" }]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;"}]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</b></p> <pre>[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;"}, {"name": "&lt;Name of Multi-Domain Log Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of R80.40 Multi-Domain Log Server&gt;"}]</pre>

Step	Instructions
	<p><b>Example</b></p> <p>There are 3 servers in the R80.30 Multi-Domain Security Management environment - the Primary Multi-Domain Server, the Secondary Multi-Domain Server, and the Multi-Domain Log Server. Both the Primary and the Secondary Multi-Domain Servers are migrated to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> <li>a. The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21</li> <li>b. The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22</li> <li>c. The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS</li> <li>d. The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS</li> <li>e. The new IPv4 address of the target Primary R80.40 Multi-Domain Server is: 172.30.40.51</li> <li>f. The new IPv4 address of the target Secondary R80.40 Multi-Domain Server is: 172.30.40.52</li> <li>g. The required syntax for the JSON configuration file you must use on both the Primary and the Secondary Multi-Domain Servers, and on the Multi-Domain Log Server:  <pre>[ {"name": "MyPrimaryMDS", "newIpAddress4": "172.30.40.51"}, {"name": "MySecondaryMDS", "newIpAddress4": "172.30.40.52"} ]</pre> </li> </ol> <p> <b>Important</b> - All servers in this environment must get this same information.</p>

## Importing the databases

**Important:**



- Make sure you followed the instructions in the above section **"Required JSON configuration file"**.
- Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line the <b>Primary</b> R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed:
	<code>cplic print</code>
	If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.
	 <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server:
	<code>md5sum /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</code>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory:
	<code>cd \$MDS_FWDIR/scripts/</code>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> <li>■ If this Multi-Domain Server is <b>not</b> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 -skip_ upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - skip_upgrade_tools_check -change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Primary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 11. Install another Secondary R80.40 Multi-Domain Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.

Step	Instructions
2	<p>Perform the clean install on another server in one of these ways:</p> <p><b>Important -</b> Do not perform initial configuration in SmartConsole.</p> <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160. Select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing a Secondary Multi-Domain Server in Management High Availability</a>" on page 72.</li> </ul>



**Important -** The IP addresses of the source and target server **can be different**. If it is necessary to have a different IP address on the target R80.40 server, you must create a special JSON configuration file before you import the management database from the source server.

Note that you have to issue licenses for the new IP address.

You must use the same JSON configuration file on all servers in the same Multi-Domain Security Management environment.

## 12. Get the required Upgrade Tools on the Secondary R80.40 Multi-Domain Server



**Note** - This step is needed only to be able to export the entire management database (for backup purposes) with the latest Upgrade Tools.



**Important -** See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.

### 13. On the Secondary R80.40 Multi-Domain Server, import the databases

#### Required JSON configuration file

If you installed the target R80.40 Multi-Domain Server with a different IP address than the source Multi-Domain Server, **you must create a special JSON configuration file before you import the management database** from the source Multi-Domain Server. Note that you have to issue licenses for the new IP address.

**Important:**



- If none of the servers in the same Multi-Domain Security Management environment changed their original IP addresses, then you do **not** need to create the special JSON configuration file.
- Even if only one of the servers migrates to a new IP address, all the other servers (including all Log Servers and SmartEvent Servers) must get this configuration file for the import process.  
**You must use the same JSON configuration file on all servers (including Log Servers and SmartEvent Servers) in the same Multi-Domain Security Management environment.**

To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R80.40 Multi-Domain Server.
2	Log in to the Expert mode.

Step	Instructions
3	<p>Create the <code>/var/log/mdss.json</code> file that contains <b>each</b> server migrated to a new IP address.</p> <p><b>Format for migrating only the Primary Multi-Domain Server to a new IP address</b></p> <pre data-bbox="493 384 1430 489">[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;" } ]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</b></p> <pre data-bbox="493 608 1430 810">[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;" }, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;" } ]</pre> <p><b>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</b></p> <pre data-bbox="493 929 1430 1244">[ {"name": "&lt;Name of Primary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Primary R80.40 Multi-Domain Server&gt;" }, {"name": "&lt;Name of Secondary Multi-Domain Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of Secondary R80.40 Multi-Domain Server&gt;" }, {"name": "&lt;Name of Multi-Domain Log Server Object in SmartConsole&gt;", "newIpAddress4": "&lt;New IPv4 Address of R80.40 Multi-Domain Log Server&gt;" } ]</pre>

Step	Instructions
	<p><b>Example</b></p> <p>There are 3 servers in the R80.30 Multi-Domain Security Management environment - the Primary Multi-Domain Server, the Secondary Multi-Domain Server, and the Multi-Domain Log Server. Both the Primary and the Secondary Multi-Domain Servers are migrated to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> <li>a. The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21</li> <li>b. The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22</li> <li>c. The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS</li> <li>d. The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS</li> <li>e. The new IPv4 address of the target Primary R80.40 Multi-Domain Server is: 172.30.40.51</li> <li>f. The new IPv4 address of the target Secondary R80.40 Multi-Domain Server is: 172.30.40.52</li> <li>g. The required syntax for the JSON configuration file you must use on both the Primary and the Secondary Multi-Domain Servers, and on the Multi-Domain Log Server:  <pre>[ {"name": "MyPrimaryMDS", "newIpAddress4": "172.30.40.51"}, {"name": "MySecondaryMDS", "newIpAddress4": "172.30.40.52"} ]</pre> </li> </ol> <p> <b>Important</b> - All servers in this environment must get this same information.</p>

## Importing the databases

### Important:



- Make sure you followed the instructions in the above section **"Required JSON configuration file"**.
- Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line the <b>Secondary R80.40 Multi-Domain Server</b> .
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed:
	<code>cplic print</code>
	If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Server, to some directory.
	 <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server:
	<code>md5sum /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</code>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory:
	<code>cd \$MDS_FWDIR/scripts/</code>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Server <i>is</i> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> <li>■ If this Multi-Domain Server is <b>not</b> connected to the Internet:           <ul style="list-style-type: none"> <li>• And none of the servers changed their IP addresses, run:               <pre>./migrate_server import -v R80.40 -skip_ upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> <li>• And at least one of the servers changed its IP address, run:               <pre>./migrate_server import -v R80.40 [-l   -x] - skip_upgrade_tools_check -change_ips_file /var/log/mdss.json /&lt;Full Path&gt;/Secondary_&lt;Name of Exported File&gt;.tgz</pre> </li> </ul> </li> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

#### 14. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Primary Multi-Domain Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Secondary Multi-Domain Server object.

Step	Instructions
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 15. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers



**Important** - If your Multi-Domain Server manages Multi-Domain Log Servers, dedicated Log Servers, or dedicated SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Multi-Domain Server.

Select the applicable upgrade option:

- For servers R80.20 and higher:
  - "*Upgrading a Multi-Domain Log Server from R80.20 and higher*" on page 430
  - "*Upgrading a Security Management Server or Log Server from R80.20 and higher*" on page 244
- For servers R80.10 and lower:
  - "*Upgrading a Multi-Domain Log Server from R80.10 and lower*" on page 409
  - "*Upgrading a Dedicated Log Server from R80.10 and lower*" on page 212
  - "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" on page 228

## 16. Install the management database on each Domain Management Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 17. Upgrade the attributes of all managed objects in all Domain Management Servers



**Important** - Perform this steps on every Multi-Domain Server with **Active** Domain Management Servers.  
To determine which Multi-Domain Servers run **Active** Domain Management Servers:

- a. Connect with SmartConsole to a Multi-Domain Server and select the **MDS** context.
- b. From the left navigation panel, click **Multi Domain > Domains**.

The table shows Domains and Multi-Domain Servers:

- Every column shows a Multi-Domain Server.
- **Active** Domain Management Servers (for a Domain) are marked with a solid black "barrel" icon.
- **Standby** Domain Management Servers (for a Domain) are marked with an empty "barrel" icon.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre>mdsenv</pre>

Step	Instructions
6	<p>Upgrade the attributes of all managed objects in all Domain Management Servers at once:</p> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre>yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>■ You can perform this action on one Multi-Domain Server at a time with this command:</li> </ul> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Multi-Domain Server&gt;</pre>
7	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 18. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	<p>Reconfigure the Log Exporter:</p> <pre>cp_log_export reconf</pre>
4	<p>Restart the Log Exporter:</p> <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

**19. Test the functionality on the Primary R80.40 Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to the <b>Primary</b> R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.
3	Test the Management High Availability functionality.

# Managing Domain Management Servers During the Upgrade Process



**Best Practice** - To not make any changes to Domain Management Server databases during the upgrade process.

If your business model cannot support management downtime during the upgrade, you can continue to manage Domain Management Servers during the upgrade process.

If you make changes to Domain Management Server databases during the upgrade process, this can create a risk of inconsistent Domain Management Server database content between instances on different Multi-Domain Servers. The synchronization process cannot resolve these database inconsistencies.

After you successfully upgrade one Multi-Domain Server, you can set its Domain Management Servers to the **Active** state, while you upgrade the others. Synchronization between the Domain Management Servers occurs after all Multi-Domain Servers are upgraded.

If, during the upgrade process, you make changes to the Domain Management Server database on different Multi-Domain Servers, the contents of these databases will be different. Because you cannot synchronize these databases, some of these changes will be lost. The Domain Management Server High Availability status appears as **Collision**.

You must decide which database version to retain and synchronize it to the other Domain Management Servers. Then you must re-enter the lost changes to the synchronized database - configure the same objects and settings again.

# Upgrading a Multi-Domain Log Server from R80.10 and lower

This section provides instructions to upgrade a Multi-Domain Log Server from R80.10 and lower:

- [\*"Upgrading a Multi-Domain Log Server from R80.10 and lower with CPUSE" on page 410\*](#)
- [\*"Upgrading a Multi-Domain Log Server from R80.10 and lower with Advanced Upgrade" on page 414\*](#)
- [\*"Upgrading a Multi-Domain Log Server from R80.10 and lower with Migration" on page 422\*](#)

For configuration information, see the [\*R80.40 Multi-Domain Security Management Administration Guide\*](#).

# Upgrading a Multi-Domain Log Server from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Log Server.

## Notes:



- To upgrade from R80.20 and higher, see "[Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE](#)" on page 431.
- This upgrade method is supported only for servers that already run Gaia Operating System.

**Important - Before you upgrade a Multi-Domain Log Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	You must upgrade your Multi-Domain Servers.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Log Server.
5	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.

**Procedure:****1. Upgrade the Multi-Domain Log Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**2. Update the version of the Multi-Domain Log Server object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

**3. Install the management database on each Domain Log Server on Multi-Domain Log Server**

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server that manages the Domain Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**4. Upgrade the attributes of all managed objects in all Domain Log Servers**

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Make sure that all the required daemons have the correct state:</p> <pre data-bbox="430 271 1441 316">mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre data-bbox="430 624 1441 759">mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 855 1441 900">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Log Servers at once:</p> <pre data-bbox="430 990 1441 1035">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> <pre data-bbox="636 1192 1441 1260">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <li>■ You can perform this action on one Domain Log Server at a time with this command:</li> <pre data-bbox="636 1349 1441 1417">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Log Server&gt;</pre> </ul>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 1529 1441 1596">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1664 1441 1731">mdsstopp mdsstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>

Step	Instructions
8	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 5. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter:
	<pre>cp_log_export reconf</pre>
4	Restart the Log Exporter:
	<pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 6. Test the functionality on the R80.40 Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

## 7. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Multi-Domain Log Server from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Log Server.



**Note** - To upgrade from R80.20 and higher, see "["Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade" on page 437](#)".

**Important** - Before you upgrade a Multi-Domain Log Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	You must upgrade your Multi-Domain Servers.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Log Server.
5	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.

**Procedure:****1. Get the R80.40 installation image**

Step	Instructions
1	Download the R80.40 Clean Install ISO file from the <a href="#">R80.40 Home Page SK</a> .
2	Transfer the R80.40 ISO file to the current server to some directory (for example, /var/log/path_to_iso/).



**Note** - Make sure to transfer the file in the binary mode.

**2. On the current Multi-Domain Log Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services: <pre>mdsstop</pre>
5	Go to the main MDS context: <pre>mdsenv</pre>
6	Mount the R80.40 ISO file: <pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO: <pre>cd /mnt/cdrom/linux/p1_install/</pre>
8	Run the installation script: <pre>./mds_setup</pre> This menu shows: <pre>(1) Run Pre-upgrade verification only [recommended before upgrade] (2) Backup current Multi-Domain Server (3) Export current Multi-Domain Server Or 'Q' to quit.</pre>

Step	Instructions
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services:  <pre>mdsstart</pre> </li> <li>b. Follow the instructions in the report.</li> <li>c. In a Management High Availability environment R77.30 and lower:            If you made changes, synchronize the Domain Management Servers immediately after these changes.            (In R80 and higher, this synchronization occurs automatically.)</li> <li>d. Stop all Check Point services again:  <pre>mdsstop</pre> </li> <li>e. Run the installation script again:  <pre>./mds_setup</pre> </li> </ol> <p>This menu shows:</p> <pre>(1) Run Pre-upgrade verification only [recommended before upgrade] (2) Backup current Multi-Domain Server (3) Export current Multi-Domain Server Or 'Q' to quit.</pre>
11	Enter <b>3</b> to export the current Multi-Domain Log Server configuration.
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): <b>/var/log</b> Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre>  <p><b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.</p>
13	<p>Make sure the export file is created in the specified directory:</p> <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>

Step	Instructions
14	Calculate the MD5 for the exported file: <pre>md5sum /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
15	Transfer the exported database from the current Multi-Domain Log Server to an external storage: <pre>/var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>  <b>Note</b> - Make sure to transfer the file in the binary mode.

### 3. Install the R80.40 Multi-Domain Log Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	Follow one of these procedures: <ul style="list-style-type: none"> <li>▪ <a href="#">"Upgrading a Multi-Domain Log Server from R80.10 and lower with CPUSE" on page 410</a></li> <li>▪ <a href="#">"Installing a Multi-Domain Log Server" on page 74</a></li> </ul>
Operating System other than Gaia	Follow this procedure: <ul style="list-style-type: none"> <li>▪ <a href="#">"Installing a Multi-Domain Log Server" on page 74</a></li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See ["Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server" on page 681](#).

### 4. On the R80.40 Multi-Domain Log Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
5	<p>Transfer the exported database from an external storage to the R80.40 Multi-Domain Log Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>
6	<p>Make sure the transferred file is not corrupted.</p> <p>Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Log Server:</p> <pre>md5sum &lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
7	<p>Import the configuration:</p> <pre>yes   nohup \$MDSDIR/scripts/mds_import.sh &lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i>.</li> </ul>
8	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 5. Update the version of the Multi-Domain Log Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .

Step	Instructions
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database on each Domain Log Server on Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server that manages the Domain Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Upgrade the attributes of all managed objects in all Domain Log Servers

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstop_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

Step	Instructions
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 271 541 300">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Log Servers at once:</p> <pre data-bbox="430 406 1251 435">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre data-bbox="636 608 1319 676">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>■ You can perform this action on one Domain Log Server at a time with this command:</li> </ul> <pre data-bbox="636 777 1389 844">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Log Server&gt;</pre>
7	<p>Allow the database synchronization to run:</p> <pre data-bbox="430 938 1251 1006">\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre data-bbox="430 1073 573 1140">mdsstopp mdssstart</pre>
	<p>For more information, see <a href="#">sk121718</a>.</p>
8	<p>Make sure that all the required daemons have the correct state:</p> <pre data-bbox="430 1275 557 1304">mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre data-bbox="430 1619 1426 1769">mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdssstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the R80.40 Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Multi-Domain Log Server from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Multi-Domain Log Server and the different target Multi-Domain Log Server.



**Note** - To upgrade from R80.20 and higher, see "["Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration" on page 446](#)".

**Important** - Before you upgrade a Multi-Domain Log Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">"Backing Up and Restoring" on page 27</a> ").
2	See the " <a href="#">"Upgrade Options and Prerequisites" on page 163</a> ".
3	You must upgrade your Multi-Domain Servers.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Log Server.
5	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.

**Procedure:****1. Get the R80.40 installation image**

Step	Instructions
1	Download the R80.40 Clean Install ISO file from the <a href="#">R80.40 Home Page SK</a> .
2	Transfer the R80.40 ISO file to the current server to some directory (for example, /var/log/path_to_iso/).



**Note** - Make sure to transfer the file in the binary mode.

**2. On the current Multi-Domain Log Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Stop all Check Point services: <pre>mdsstop</pre>
5	Go to the main MDS context: <pre>mdsenv</pre>
6	Mount the R80.40 ISO file: <pre>mount -o loop /var/log/path_to_iso/&lt;R80.40_Gaia&gt;.iso /mnt/cdrom</pre>
7	Go to the installation folder in the ISO: <pre>cd /mnt/cdrom/linux/p1_install/</pre>
8	Run the installation script: <pre>./mds_setup</pre> This menu shows: <pre>(1) Run Pre-upgrade verification only [recommended before upgrade] (2) Backup current Multi-Domain Server (3) Export current Multi-Domain Server Or 'Q' to quit.</pre>

Step	Instructions
9	<p>Enter <b>1</b> to run the Pre-Upgrade Verifier.</p>  <p><b>Note</b> - The Pre-Upgrade Verifier analyzes compatibility of the currently installed configuration with the version, to which you upgrade. A detailed report shows the steps to do before and after the upgrade.</p>
10	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Start all Check Point services:  <pre>mdsstart</pre> </li> <li>b. Follow the instructions in the report.</li> <li>c. In a Management High Availability environment R77.30 and lower:            If you made changes, synchronize the Domain Management Servers immediately after these changes.            (In R80 and higher, this synchronization occurs automatically.)</li> <li>d. Stop all Check Point services again:  <pre>mdsstop</pre> </li> <li>e. Run the installation script again:  <pre>./mds_setup</pre> </li> </ol> <p>This menu shows:</p> <pre>(1) Run Pre-upgrade verification only [recommended before upgrade] (2) Backup current Multi-Domain Server (3) Export current Multi-Domain Server Or 'Q' to quit.</pre>
11	Enter <b>3</b> to export the current Multi-Domain Log Server configuration.
12	<p>Answer the interactive questions:</p> <pre>Would you like to proceed with the export now [yes/no] ? <b>yes</b> Please enter target directory for your Multi-Domain Server export (or 'Q' to quit): <b>/var/log</b> Do you plan to import to a version newer than R80.40 [yes/no] ? <b>no</b> Using migrate_tools from disk. Do you wish to export the log database [yes/no] ? <b>yes</b></pre>  <p><b>Note</b> - If you enter <b>no</b> in the question "Do you wish to export the log database", the configuration is still exported.</p>
13	<p>Make sure the export file is created in the specified directory:</p> <pre>ls -l /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>

Step	Instructions
14	Calculate the MD5 for the exported file: <pre>md5sum /var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
15	Transfer the exported database from the current Multi-Domain Log Server to an external storage: <pre>/var/log/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>  <b>Note</b> - Make sure to transfer the file in the binary mode.

### 3. Install another R80.40 Multi-Domain Log Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install on another server in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing a Multi-Domain Log Server</a>" on page 74.</li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "[Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server](#)" on page 681.

### 4. On the R80.40 Multi-Domain Log Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <pre>cplic print</pre> If it is not already installed, then install a valid license now.

Step	Instructions
5	<p>Transfer the exported database from an external storage to the R80.40 Multi-Domain Log Server, to some directory.</p>  <b>Note</b> - Make sure to transfer the file in the binary mode.
6	<p>Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Log Server:</p> <pre data-bbox="436 572 1349 617">md5sum &lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz</pre>
7	<p>Import the configuration:</p> <pre data-bbox="436 707 1246 774">yes   nohup \$MDSDIR/scripts/mds_import.sh &lt;Full Path&gt;/exported_mds.&lt;DDMMYYYY-HHMMSS&gt;.tgz &amp;</pre>
8	<p><b>Notes:</b></p>  <ul data-bbox="579 819 1421 932" style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i>.</li> </ul> <p>Make sure that all the required daemons have the correct state:</p> <pre data-bbox="436 1021 563 1044">mdsstat</pre> <ul data-bbox="460 1066 1413 1235" style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre data-bbox="436 1358 1421 1493">mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 5. Update the version of the Multi-Domain Log Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click <b>General</b> .

Step	Instructions
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database on each Domain Log Server on Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server that manages the Domain Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Upgrade the attributes of all managed objects in all Domain Log Servers

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre>mdsenv</pre>

Step	Instructions
6	<p>Upgrade the attributes of all managed objects in all Domain Log Servers at once:</p> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre>yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>■ You can perform this action on one Domain Log Server at a time with this command:</li> </ul> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Log Server&gt;</pre>
7	<p>Allow the database synchronization to run:</p> <pre>\$CPDIR/bin/cpprod_util CPPROD_SetValue "FW1/6.0" AfterUpgradeDbsyncIndication 1 1 0</pre> <p>Restart the Check Point services:</p> <pre>mdsstopp mdssstart</pre> <p>For more information, see <a href="#">sk121718</a>.</p>
8	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdssstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the R80.40 Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server.
2	Make sure the management database and configuration were upgraded correctly.

## 11. Disconnect the old Multi-Domain Log Server from the network

Disconnect the network cables the old Multi-Domain Log Server.

## 12. Connect the new Multi-Domain Log Server to the network

Connect the network cables to the new Multi-Domain Log Server.

# Upgrading a Multi-Domain Log Server from R80.20 and higher

This section provides instructions to upgrade a Multi-Domain Log Server from R80.20.M1, R80.20, R80.20.M2, or R80.30:

- [\*"Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE" on page 431\*](#)
- [\*"Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade" on page 437\*](#)
- [\*"Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration" on page 446\*](#)

For additional information related to these upgrade procedures, see [sk163814](#).

For configuration information, see the [\*R80.40 Multi-Domain Security Management Administration Guide\*](#).

# Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Log Server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Multi-Domain Log Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	You must upgrade your Multi-Domain Servers.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Log Server.
5	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.

**Procedure:****1. Get the required Upgrade Tools on the server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>.            (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE.            See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.            Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. Upgrade the Multi-Domain Log Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on [page 160](#) and follow the applicable action plan.

**3. Update the version of the Multi-Domain Log Server object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.

Step	Instructions
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

#### 4. Install the management database on each Domain Log Server on Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server that manages the Domain Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

#### 5. Upgrade the attributes of all managed objects in all Domain Log Servers

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	<p>Make sure that all the required daemons have the correct state:</p> <pre data-bbox="430 271 1441 316">mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre data-bbox="430 624 1441 759">mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre data-bbox="430 855 1441 900">mdsenv</pre>
6	<p>Upgrade the attributes of all managed objects in all Domain Log Servers at once:</p> <pre data-bbox="430 983 1441 1028">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:       <pre data-bbox="636 1192 1441 1260">yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> </li> <li>■ You can perform this action on one Domain Log Server at a time with this command:       <pre data-bbox="636 1349 1441 1417">\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Log Server&gt;</pre> </li> </ul>

Step	Instructions
7	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 6. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter:
	<pre>cp_log_export reconf</pre>
4	Restart the Log Exporter:
	<pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 7. Test the functionality on the R80.40 Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

## 8. Test the functionality on the R80.40 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	Make sure the logging works as expected.

# Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Multi-Domain Log Server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important** - Before you upgrade a Multi-Domain Log Server:



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	You must upgrade your Multi-Domain Servers.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Log Server.
5	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Multi-Domain Log Server, run the Pre-Upgrade Verifier and export the**

## entire management database

Step	Instructions
1	Connect to the command line on the current Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>
6	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the source Multi-Domain Log Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Multi-Domain Log Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing a Multi-Domain Log Server</a>" on page 74.</li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "[Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server](#)" on page 681.

### 4. Get the required Upgrade Tools on the R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a> . (See " <a href="#">Management Server Migration Tool and Upgrade Tools</a> " on page 182.) <b>Note</b> - This is a CPUSE Offline package.
2	Install the R80.40 Upgrade Tools with CPUSE. See " <a href="#">Installing Software Packages on Gaia</a> " on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.
3	Make sure the package is installed. Run this command in the Expert mode: <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. <b>Example</b> Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

## 5. On the R80.40 Multi-Domain Log Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Log Server, to some directory.   <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> </div>
7	Go to the \$MDS_FWDIR/scripts/ directory: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cd \$MDS_FWDIR/scripts/</pre> </div>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run:</li> </ul> <pre data-bbox="504 309 1362 377">./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is not</i> connected to the Internet, run:</li> </ul> <pre data-bbox="504 444 1399 541">./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons have the correct state:</p> <pre data-bbox="435 714 562 741">mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre data-bbox="435 1064 1422 1192">mdsstop_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Update the version of the Multi-Domain Log Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 8. Install the management database on each Domain Log Server on Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server that manages the Domain Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 9. Upgrade the attributes of all managed objects in all Domain Log Servers

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre>mdsenv</pre>

Step	Instructions
6	<p>Upgrade the attributes of all managed objects in all Domain Log Servers at once:</p> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre>yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>You can perform this action on one Domain Log Server at a time with this command:</li> </ul> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Log Server&gt;</pre>
7	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>The state of the CPC daemon must be "N/R" on the MDS level.</li> <li>The state of the CPC daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 10. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	<p>Reconfigure the Log Exporter:</p> <pre>cp_log_export reconf</pre>
4	<p>Restart the Log Exporter:</p> <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

**11. Test the functionality on the R80.40 Multi-Domain Log Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

**12. Test the functionality on the R80.40 Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	Make sure the logging works as expected.

# Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration

In a migration and upgrade scenario, you perform the procedure on the source Multi-Domain Server and the different target Multi-Domain Server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important - Before you upgrade a Multi-Domain Log Server:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	You must upgrade your Multi-Domain Servers.
4	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Log Server.
5	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "*Management Server Migration Tool and Upgrade Tools*" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<i>Management Server Migration Tool and Upgrade Tools</i>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<i>Installing Software Packages on Gaia</i>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Multi-Domain Log Server, run the Pre-Upgrade Verifier and export the**

## entire management database

Step	Instructions
1	Connect to the command line on the current Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>a. Follow the instructions in the report.</li> <li>b. Run the Pre-Upgrade Verifier again.</li> </ol>
6	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre>cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <b>is not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the source Multi-Domain Log Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install another R80.40 Multi-Domain Log Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform the clean install on another server in one of these ways (do <b>not</b> perform initial configuration in SmartConsole): <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing a Multi-Domain Log Server</a>" on page 74.</li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. See "[Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server](#)" on page 681.

### 4. Get the required Upgrade Tools on the R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a> . (See " <a href="#">Management Server Migration Tool and Upgrade Tools</a> " on page 182.) <b>Note</b> - This is a CPUSE Offline package.
2	Install the R80.40 Upgrade Tools with CPUSE. See " <a href="#">Installing Software Packages on Gaia</a> " on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.
3	Make sure the package is installed. Run this command in the Expert mode: <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. <b>Example</b> Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

## 5. On the R80.40 Multi-Domain Log Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R80.40 Multi-Domain Log Server, to some directory.   <b>Note</b> - Make sure to transfer the file in the binary mode.
6	Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original Multi-Domain Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> </div>
7	Go to the \$MDS_FWDIR/scripts/ directory: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cd \$MDS_FWDIR/scripts/</pre> </div>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run:</li> </ul> <pre data-bbox="504 309 1362 377">./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Multi-Domain Log Server <i>is not</i> connected to the Internet, run:</li> </ul> <pre data-bbox="504 444 1399 541">./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>
9	<p>Make sure that all the required daemons have the correct state:</p> <pre data-bbox="435 714 562 741">mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre data-bbox="435 1064 1422 1192">mdsstop_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Update the version of the Multi-Domain Log Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click <b>General</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 8. Install the management database on each Domain Log Server on Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to each Domain Management Server that manages the Domain Log Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 9. Upgrade the attributes of all managed objects in all Domain Log Servers

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Log Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>■ The state of the CPCDA daemon must be "N/R" on the MDS level.</li> <li>■ The state of the CPCDA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>
5	<p>Go to the main MDS context:</p> <pre>mdsenv</pre>

Step	Instructions
6	<p>Upgrade the attributes of all managed objects in all Domain Log Servers at once:</p> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>Because the command prompts you for a 'yes/no' for each Domain and each object in the Domain, you can explicitly provide the 'yes' answer to all questions with this command:</li> </ul> <pre>yes   \$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL</pre> <ul style="list-style-type: none"> <li>You can perform this action on one Domain Log Server at a time with this command:</li> </ul> <pre>\$MDSDIR/scripts/mds_fix_cmas_clms_version -c ALL -n &lt;Name of Domain Log Server&gt;</pre>
7	<p>Make sure that all the required daemons have the correct state:</p> <pre>mdsstat</pre> <ul style="list-style-type: none"> <li>The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd".</li> <li>The state of the CPCA daemon must be "N/R" on the MDS level.</li> <li>The state of the CPCA daemon must be "down" on the Domain Log Server level.</li> </ul> <p>If the state of one of the required daemons (FWM, FWD, or CPD) on a Domain Log Server is "down", then wait for 5-10 minutes, restart that Domain Log Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Log Server&gt; mdsstat</pre>

## 10. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	<p>Reconfigure the Log Exporter:</p> <pre>cp_log_export reconf</pre>
4	<p>Restart the Log Exporter:</p> <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

**11. Test the functionality on the R80.40 Multi-Domain Log Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

**12. Test the functionality on the R80.40 Multi-Domain Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Multi-Domain Server that manages the Multi-Domain Log Server.
2	Make sure the logging works as expected.

**13. Disconnect the old Multi-Domain Log Server from the network**

Disconnect the network cables the old Multi-Domain Log Server.

**14. Connect the new Multi-Domain Log Server to the network**

Connect the network cables to the new Multi-Domain Log Server.

# Upgrade of Endpoint Security Management Servers and Endpoint Policy Servers

This section provides instructions to upgrade Endpoint Security Management Servers and Endpoint Policy Servers:

- [\*"Upgrading an Endpoint Security Management Server from R80.10 and lower" on page 456\*](#)
- [\*"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482\*](#)
- [\*"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher" on page 499\*](#)

# Upgrading an Endpoint Security Management Server from R80.10 and lower

This section provides instructions to upgrade Security Management Servers, Endpoint Security Management Server, or vSEC Controller R80.10 and lower:

- [\*"Upgrading an Endpoint Security Management Server from R80.10 and lower with CPUSE" on page 457\*](#)
- [\*"Upgrading an Endpoint Security Management Server from R80.10 and lower with Advanced Upgrade" on page 460\*](#)
- [\*"Upgrading an Endpoint Security Management Server from R80.10 and lower with Migration" on page 470\*](#)
- [\*"Upgrading Endpoint Security Management Servers in Management High Availability from R80.10 and lower" on page 477\*](#)

# Upgrading an Endpoint Security Management Server from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Endpoint Security Management Server.

**Notes:**



- To upgrade from R80.20 and higher, see "["Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE" on page 500](#)".
- This upgrade method is supported only for servers that already run on Gaia Operating System.

**Important - Before you upgrade an Endpoint Security Management Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	<p>In R80 and higher, examine the SmartConsole sessions:</p> <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Endpoint Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server.

**Procedure:****1. Upgrade the Endpoint Security Management Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**2. Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on page 89.

**3. Upgrade the dedicated Endpoint Policy Servers**

If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must upgrade these dedicated servers to the same version as the Endpoint Security Management Server:

["Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482](#)

If applicable, see:

- ["Upgrading a Dedicated Log Server from R80.10 and lower" on page 212](#)
- ["Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228](#)

**4. Install the management database**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**5. Install the Event Policy**

**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Endpoint Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.

Step	Instructions
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 6. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 7. Test the functionality on the R80.40 Endpoint Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading an Endpoint Security Management Server from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Endpoint Security Management Server.



**Note** - To upgrade from R80.20 and higher, see "["Upgrading an Endpoint Security Management Server from R80.10 and lower with Advanced Upgrade"](#) above.

**Important** - Before you upgrade an Endpoint Security Management Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"><li>Connect with the SmartConsole to the Endpoint Security Management Server.</li><li>From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li><li>You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li></ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current Endpoint Security Management Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Endpoint Security Management Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ You can also export the MSI packages with the "<b>--include-uepm-msi-files</b>" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <b>Security Management Server Commands</b> - Section <i>migrate</i>.</li> </ul>
7	 <p><b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Endpoint Security Management Server, then export the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the current Endpoint Security Management Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install the R80.40 Endpoint Security Management Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading an Endpoint Security Management Server from R80.10 and lower" on page 456</a></li> <li>■ <a href="#">"Installing an Endpoint Security Management Server" on page 77</a></li> </ul>
Operating System other than Gaia	<p>Follow this procedure:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing an Endpoint Security Management Server" on page 77</a></li> </ul>

**Important:**

- If you upgrade from R80 (or higher) version to R80.40, then these options are available:
  - The IP addresses of the source and target Endpoint Security Management Servers **can be the same**.  
If in the future it is necessary to have a different IP address on the R80.40 Endpoint Security Management Server, you can change it. For applicable procedures, see [sk40993](#) and [sk65451](#).  
Note that you have to issue licenses for the new IP address.
  - The IP addresses of the source and target Endpoint Security Management Servers **can be different**.  
Note that you have to issue licenses for the new IP address.  
You must install the new licenses only after you import the databases.
- If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Endpoint Security Management Servers **must be the same**.  
If it is necessary to have a different IP address on the R80.40 Endpoint Security Management Server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.

**4. On the R80.40 Endpoint Security Management Server, import the databases**

**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Endpoint Security Management Server.
2	Log in to the Expert mode.
3	Make sure a valid license is installed: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cplic print</pre> </div> If it is not already installed, then install a valid license now.
4	Transfer the exported databases from an external storage to the R80.40 Endpoint Security Management Server, to some directory. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <b>Note</b> - Make sure to transfer the files in the binary mode.         </div>
5	Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Endpoint Security Management Server: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> </div>
6	Go to the \$FWDIR/bin/upgrade_tools/ directory: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cd \$FWDIR/bin/upgrade_tools/</pre> </div>

Step	Instructions
7	<p>Import the management database:</p> <pre data-bbox="441 271 1287 339">yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre>
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ You can also import the MSI packages with the "<code>--include-uepm-msi-files</code>" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate</i>.</li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ If you upgrade from R80 (or higher) version, and the IP addresses of the source and target Endpoint Security Management Servers <b>are different</b>:       <ol style="list-style-type: none"> <li>Issue licenses for the new IP address in your Check Point User Center account.</li> <li>Install the new licenses on the R80.40 Endpoint Security Management Server.</li> </ol> </li> <li>■ If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Endpoint Security Management Servers <b>must be the same</b>.       <ul style="list-style-type: none"> <li>• If it is necessary to have a different IP address on the R80.40 Endpoint Security Management Server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.</li> </ul> </li> </ul>
8	 <p><b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Endpoint Security Management Server, then import the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
9	<p>Restart the Check Point services:</p> <pre data-bbox="441 1500 562 1567">cpstop cpstart</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Install the licenses and change the IP address of the R80.40 Endpoint Security Management Server

Scenario	Instructions
You upgraded from R80 (or higher) version to R80.40, and the IP addresses of the source and target Endpoint Security Management Servers <b>are different</b>	<p>Follow these steps:</p> <ol style="list-style-type: none"><li data-bbox="976 258 1453 370">Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.</li><li data-bbox="976 370 1421 482">Install the new licenses on the R80.40 Endpoint Security Management Server.</li></ol>

Scenario	Instructions
<p>You upgraded from R77.30 (and lower) version to R80.40 and need to have a different IP address on the R80.40 Endpoint Security Management Servers</p>	<p>Follow these steps (based on <a href="#">sk40993</a>):</p> <ul style="list-style-type: none"> <li>a. Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.</li> <li>b. Perform the required changes in the SmartConsole: <ul style="list-style-type: none"> <li>i. Connect with SmartConsole to the Endpoint Security Management Servers.</li> <li>ii. From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>iii. Open the Endpoint Security Management Servers object.</li> <li>iv. On the <b>General Properties</b> page, change the current IP address to the new IP address.</li> <li>v. On the <b>Network Management</b> page, edit the applicable interface and change the current IP address to the new IP address.</li> <li>vi. Click <b>OK</b>.</li> <li>vii. Publish the SmartConsole session.</li> <li>viii. Close the SmartConsole.</li> </ul> </li> <li>c. Stop the Check Point services: <ul style="list-style-type: none"> <li>i. Connect to the command line.</li> <li>ii. Log in to either Gaia Clish, or Expert mode.</li> <li>iii. Run: <code>cpstop</code></li> </ul> </li> <li>d. Perform the required changes in Gaia OS: <ul style="list-style-type: none"> <li>i. Connect to either Gaia Portal, or Gaia Clish.</li> <li>ii. Edit the applicable interface and change the current IP address to the new IP address.</li> </ul> </li> </ul> <p>You can perform this change in either Gaia Portal, or Gaia Clish. For details, see <a href="#">R80.40 Gaia Administration Guide</a>.</p>

Scenario	Instructions
	 <b>Note</b> - If this Endpoint Security Management Servers has only one interface, then your HTTPS and SSH connection to this Endpoint Security Management Servers is interrupted when you change its IP address. You need to connect again. To avoid this interruption, connect to the Endpoint Security Management Servers over the serial console. <ul style="list-style-type: none"> <li data-bbox="986 765 1446 968">e. Install the new licenses on the R80.40 Endpoint Security Management Servers. You can do this either in the CLI with the "cplic put" command, or in the Gaia Portal.</li> <li data-bbox="986 979 1446 1192">f. Start the Check Point services: <ul style="list-style-type: none"> <li data-bbox="1065 1012 1430 1080">i. Connect to the command line.</li> <li data-bbox="1065 1091 1430 1158">ii. Log in to either Gaia Clish, or the Expert mode.</li> <li data-bbox="1065 1170 1303 1192">iii. Run: cpstart</li> </ul> </li> </ul>

## 7. Upgrade the dedicated Endpoint Policy Servers

This step is part of the upgrade procedure of a Endpoint Security Management Server server. If you upgrade a dedicated Endpoint Policy Server, then skip this step.

If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must upgrade these dedicated servers to the same version as the Endpoint Security Management Server:

["Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482](#)

If applicable, see:

- ["Upgrading a Dedicated Log Server from R80.10 and lower" on page 212](#)
- ["Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228](#)

## 8. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.

Step	Instructions
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 9. Install the Event Policy



**Important -** This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Endpoint Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 10. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 11. Test the functionality on the R80.40 Endpoint Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading an Endpoint Security Management Server from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Endpoint Security Management Server and the different target Endpoint Security Management Server.



**Note** - To upgrade from R80.20 and higher, see "[Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration](#)" on page 513.

**Important** - Before you upgrade an Endpoint Security Management Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>Connect with the SmartConsole to the Endpoint Security Management Server.</li> <li>From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current Endpoint Security Management Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Endpoint Security Management Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ You can also export the MSI packages with the "<b>--include-uepm-msi-files</b>" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <b>Security Management Server Commands</b> - Section <i>migrate</i>.</li> </ul>
7	<p> <b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Endpoint Security Management Server, then export the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the current Endpoint Security Management Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Endpoint Security Management Server

Perform a clean install of the R80.40 Endpoint Security Management Server on another computer.

Do **not** perform initial configuration in SmartConsole.

See "[Installing an Endpoint Security Management Server](#)" on page 77.



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 Endpoint Security Management Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Endpoint Security Management Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre data-bbox="425 415 632 449">cplic print</pre>
	If it is not already installed, then install a valid license now.
4	<p>Transfer the exported databases from an external storage to the R80.40 Endpoint Security Management Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the files in the binary mode.</p>
5	<p>Make sure the transferred files are not corrupted.</p> <p>Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Endpoint Security Management Server:</p>
	<pre data-bbox="425 878 1235 911">md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/bin/upgrade_tools/ directory:</p> <pre data-bbox="425 1021 917 1055">cd \$FWDIR/bin/upgrade_tools/</pre>
7	<p>Import the management database:</p> <pre data-bbox="425 1156 1287 1224">yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre>  <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ You can also import the MSI packages with the "<b>--include-uepm-msi-files</b>" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate</i>.</li> </ul>

Step	Instructions
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ If you upgrade from R80 (or higher) version, and the IP addresses of the source and target Endpoint Security Management Servers <b>are different</b>:             <ol style="list-style-type: none"> <li>a. Issue licenses for the new IP address in your Check Point User Center account.</li> <li>b. Install the new licenses on the R80.40 Endpoint Security Management Server.</li> </ol> </li> <li>■ If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Endpoint Security Management Servers <b>must be the same</b>.             <ul style="list-style-type: none"> <li>• If it is necessary to have a different IP address on the R80.40 Endpoint Security Management Server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.</li> </ul> </li> </ul>
8	 <p><b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Endpoint Security Management Server, then import the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
9	<p>Restart the Check Point services:</p> <pre>cpstop cpstart</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Upgrade the dedicated Endpoint Policy Servers

This step is part of the upgrade procedure of a Endpoint Security Management Server server. If you upgrade a dedicated Endpoint Policy Server, then skip this step.

If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must upgrade these dedicated servers to the same version as the Endpoint Security Management Server:

["Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482](#)

If applicable, see:

- ["Upgrading a Dedicated Log Server from R80.10 and lower" on page 212](#)
- ["Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228](#)

## 7. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 8. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Endpoint Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 9. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 10. Test the functionality on the R80.40 Endpoint Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

## 11. Disconnect the old Endpoint Security Management Server from the network

Disconnect the network cables the old Endpoint Security Management Server.

## 12. Connect the new Endpoint Security Management Server to the network

Connect the network cables to the new Endpoint Security Management Server.

# Upgrading Endpoint Security Management Servers in Management High Availability from R80.10 and lower

**Important** - Before you upgrade an Endpoint Security Management Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>Connect with the SmartConsole to the Endpoint Security Management Server.</li> <li>From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server.



**Important** - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.

## Upgrading from R80 or higher versions

Step	Instructions
1	Upgrade the <b>Primary</b> Endpoint Security Management Server with one of the supported methods. See " <a href="#">Upgrade Methods</a> " on page 175.
2	Upgrade the <b>Secondary</b> Endpoint Security Management Server with one of the supported methods. See " <a href="#">Upgrade Methods</a> " on page 175.
3	Get the R80.40 SmartConsole. See " <a href="#">Installing SmartConsole</a> " on page 89.
4	Connect with R80.40 SmartConsole to the R80.40 Primary Endpoint Security Management Server.
5	Update the object version of the Secondary Endpoint Security Management Server: <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Endpoint Security Management Server object.</li> <li>From the left tree, click <b>General Properties</b>.</li> <li>In the <b>Platform</b> section &gt; in the <b>Version</b> field, select <b>R80.40</b>.</li> <li>Click <b>OK</b>.</li> </ol>

Step	Instructions
6	<p>Make sure Secure Internal Communication (SIC) works correctly with the Secondary Endpoint Security Management Server:</p> <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Endpoint Security Management Server object.</li> <li>On the <b>General Properties</b> page, click <b>Communication</b>.</li> <li>Click <b>Test SIC Status</b>. The SIC Status must show <b>Communicating</b>.</li> <li>Click <b>Close</b>.</li> <li>Click <b>OK</b>.</li> </ol>
7	<p>Install the management database:</p> <ol style="list-style-type: none"> <li>In the top left corner, click <b>Menu &gt; Install database</b>.</li> <li>Select all objects.</li> <li>Click <b>Install</b>.</li> <li>Click <b>OK</b>.</li> </ol>
8	<p>Install the Event Policy.</p> <p> <b>Important</b> - This step applies only if the <b>SmartEvent Correlation Unit Software Blade</b> is enabled on the R80.40 Endpoint Security Management Server.</p> <ol style="list-style-type: none"> <li>In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b>.</li> <li>At the top, click <b>+</b> to open a new tab.</li> <li>In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b>. The Legacy SmartEvent client opens.</li> <li>In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b>.</li> <li>Confirm.</li> <li>Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded</li> <li>Click <b>Close</b>.</li> <li>Close the Legacy SmartEvent client.</li> </ol>
9	<p>Reconfigure the Log Exporter:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the server.</li> <li>Log in to the Expert mode.</li> <li>Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre></li> <li>Restart the Log Exporter: <pre>cp_log_export restart</pre></li> </ol> <p>For more information, see the <a href="#">R80.40 Logging and Monitoring Administration Guide</a> &gt; Chapter <i>Log Exporter</i></p>

Step	Instructions
10	<p>Synchronize the Endpoint Security Management Servers:</p> <ol style="list-style-type: none"><li>a. In the top left corner, click <b>Menu &gt; Management High Availability</b>.</li><li>b. In the <b>Peers</b> section, click <b>Actions &gt; Sync Peer</b>.</li><li>c. The status must show <b>Successfully synced</b> for all peers.</li></ol>

## Upgrading from R77.30 and lower versions

Step	Instructions
1	Upgrade the <b>Primary</b> Endpoint Security Management Server with one of the supported methods. See " <a href="#">Upgrade Methods</a> " on page 175.
2	Perform a <i>clean install</i> of the R80.40 on the Secondary Endpoint Security Management Server. See " <a href="#">Installing a Secondary Endpoint Security Management Server in Management High Availability</a> " on page 79.
3	Get the R80.40 SmartConsole. See " <a href="#">Installing SmartConsole</a> " on page 89.
4	Connect with R80.40 SmartConsole to the R80.40 Primary Endpoint Security Management Server.
5	Update the object version of the Secondary Endpoint Security Management Server: <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Endpoint Security Management Server object.</li> <li>From the left tree, click <b>General Properties</b>.</li> <li>In the <b>Platform</b> section &gt; in the <b>Version</b> field, select <b>R80.40</b>.</li> <li>Click <b>OK</b>.</li> </ol>
6	Make sure Secure Internal Communication (SIC) works correctly with the Secondary Endpoint Security Management Server: <ol style="list-style-type: none"> <li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>Open the Secondary Endpoint Security Management Server object.</li> <li>On the <b>General Properties</b> page, click <b>Communication</b>.</li> <li>Click <b>Test SIC Status</b>. The SIC Status must show <b>Communicating</b>.</li> <li>Click <b>Close</b>.</li> <li>Click <b>OK</b>.</li> </ol>
7	Install the management database: <ol style="list-style-type: none"> <li>In the top left corner, click <b>Menu &gt; Install database</b>.</li> <li>Select all objects.</li> <li>Click <b>Install</b>.</li> <li>Click <b>OK</b>.</li> </ol>

Step	Instructions
8	<p>Install the Event Policy.</p>  <p><b>Important</b> - This step applies only if the <b>SmartEvent Correlation Unit Software Blade</b> is enabled on the R80.40 Endpoint Security Management Server.</p> <ol style="list-style-type: none"> <li>a. In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b>.</li> <li>b. At the top, click <b>+</b> to open a new tab.</li> <li>c. In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b>. The Legacy SmartEvent client opens.</li> <li>d. In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b>.</li> <li>e. Confirm.</li> <li>f. Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded</li> <li>g. Click <b>Close</b>.</li> <li>h. Close the Legacy SmartEvent client.</li> </ol>
9	<p>Reconfigure the Log Exporter:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the server.</li> <li>b. Log in to the Expert mode.</li> <li>c. Reconfigure the Log Exporter:  <pre>cp_log_export reconf</pre> </li> <li>d. Restart the Log Exporter:  <pre>cp_log_export restart</pre> </li> </ol> <p>For more information, see the <a href="#">R80.40 Logging and Monitoring Administration Guide</a> &gt; Chapter Log Exporter</p> <p>Synchronize the Endpoint Security Management Servers:</p> <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Management High Availability</b>.</li> <li>b. In the <b>Peers</b> section, click <b>Actions &gt; Sync Peer</b>.</li> <li>c. The status must show <b>Successfully synced</b> for all peers.</li> </ol>

# Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower

This section provides instructions to upgrade dedicated Endpoint Policy Servers:

- [\*"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with CPUSE" on page 483\*](#)
- [\*"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Advanced Upgrade" on page 487\*](#)
- [\*"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Migration" on page 493\*](#)

# Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same dedicated Endpoint Policy Server.

## Notes:



- To upgrade from R80.20 and higher, see "["Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE" on page 500](#)".
- This upgrade method is supported only for servers that already run on Gaia Operating System.

**Important - Before you upgrade a dedicated Endpoint Policy Server:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Before you upgrade a dedicated Endpoint Policy Server, you must upgrade the applicable Endpoint Security Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the Endpoint Policy Server.

**Procedure:****1. Upgrade the dedicated Endpoint Policy Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**2. Update the version of the Endpoint Policy Server object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

**3. Install the management database**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server that manages the dedicated Endpoint Policy Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**4. Install the Event Policy on the dedicated Endpoint Policy Server**

**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the dedicated R80.40 Endpoint Policy Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Policy Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.

Step	Instructions
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 5. Test the functionality on the dedicated Endpoint Policy Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 Endpoint Policy Server.
2	Make sure the management database and configuration were upgraded correctly.

## 6. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 7. Test the functionality on the dedicated Endpoint Policy Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 Endpoint Policy Server.
2	Make sure the management database and configuration were upgraded correctly.

**8. Test the functionality on the R80.40 Endpoint Security Management Server**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server that manages the dedicated Endpoint Policy Server.
2	Make sure everything works as expected.

# Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same dedicated Endpoint Policy Server.



**Notes** - To upgrade from R80.20 and higher, see "*Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade*" on page 505.

**Important** - Before you upgrade a dedicated Endpoint Policy Server:

Step	Instructions
1	Back up your current configuration (see " <i>Backing Up and Restoring</i> " on page 27).
2	See the " <i>Upgrade Options and Prerequisites</i> " on page 163.
3	Before you upgrade a dedicated Endpoint Policy Server, you must upgrade the applicable Endpoint Security Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the Endpoint Policy Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current dedicated Endpoint Policy Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current dedicated Endpoint Policy Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Endpoint Security Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	<p>Transfer the exported databases from the current server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install the R80.40 Endpoint Policy Server

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482</a></li> <li>■ <a href="#">"Installing an Endpoint Policy Server" on page 82</a></li> </ul>
Operating System other than Gaia	<p>Follow this procedure:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing an Endpoint Policy Server" on page 82</a></li> </ul>



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 or Endpoint Policy Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Endpoint Policy Server.

Step	Instructions
2	Log in to the Expert mode.
3	Make sure a valid license is installed: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
4	Transfer the exported databases from an external storage to the R80.40 or Endpoint Policy Server, to some directory.  <b>Note</b> - Make sure to transfer the files in the binary mode.
5	Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Endpoint Policy Server: <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	Go to the \$FWDIR/bin/upgrade_tools/ directory: <pre>cd \$FWDIR/bin/upgrade_tools/</pre>
7	Import the management database: <pre>yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre>  <b>Notes:</b> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
8	Restart the Check Point services: <pre>cpstop cpstart</pre>

## 5. Update the version of the Endpoint Policy Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click <b>General Properties</b> .

Step	Instructions
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server that manages the dedicated Endpoint Policy Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy on the dedicated Endpoint Policy Server



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the dedicated R80.40 Endpoint Policy Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Policy Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the dedicated Endpoint Policy Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 Endpoint Policy Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Endpoint Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server that manages the dedicated Endpoint Policy Server.
2	Make sure everything works as expected.

# Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Endpoint Policy Server and the different target Endpoint Policy Server.



**Notes** - To upgrade from R80.20 and higher, see "*Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration*" on page 513.

**Important** - Before you upgrade a dedicated Endpoint Policy Server:

Step	Instructions
1	Back up your current configuration (see " <i>Backing Up and Restoring</i> " on page 27).
2	See the " <i>Upgrade Options and Prerequisites</i> " on page 163.
3	Before you upgrade a dedicated Endpoint Policy Server, you must upgrade the applicable Endpoint Security Management Server that manages it.
4	You must close all GUI clients (SmartConsole applications) connected to the Endpoint Policy Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current dedicated Endpoint Policy Server, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current dedicated Endpoint Policy Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Endpoint Security Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
8	<p>Transfer the exported databases from the current server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Endpoint Policy Server

Perform a clean install of the R80.40 Endpoint Policy Server on another computer.

Do **not** perform initial configuration in SmartConsole.

See "[Installing an Endpoint Policy Server](#)" on page 82



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 4. On the R80.40 or Endpoint Policy Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Endpoint Policy Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>

Step	Instructions
4	<p>Transfer the exported databases from an external storage to the R80.40 or Endpoint Policy Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the files in the binary mode.</p>
5	<p>Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Endpoint Policy Server:</p> <pre data-bbox="430 563 1235 597">md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/bin/upgrade_tools/ directory:</p> <pre data-bbox="430 687 917 720">cd \$FWDIR/bin/upgrade_tools/</pre>
7	<p>Import the management database:</p> <pre data-bbox="430 822 1287 889">yes   nohup ./migrate import [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ yes   nohup ... &amp; are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
8	<p>Restart the Check Point services:</p> <pre data-bbox="430 1136 557 1203">cpstop cpstart</pre>

## 5. Update the version of the Endpoint Policy Server object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server that manages the dedicated Endpoint Policy Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy on the dedicated Endpoint Policy Server



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the dedicated R80.40 Endpoint Policy Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Policy Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 9. Test the functionality on the dedicated Endpoint Policy Server

Step	Instructions
1	Connect with SmartConsole to the dedicated R80.40 Endpoint Policy Server.
2	Make sure the management database and configuration were upgraded correctly.

## 10. Test the functionality on the R80.40 Endpoint Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server that manages the dedicated Endpoint Policy Server.
2	Make sure everything works as expected.

# Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher

This section provides instructions to upgrade Security Management Servers and dedicated Log Servers from R80.20.M1, R80.20, R80.20.M2, or R80.30:

- [\*"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE" on page 500\*](#)
- [\*"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade" on page 505\*](#)
- [\*"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration" on page 513\*](#)
- [\*"Upgrading Endpoint Security Management Servers in Management High Availability from R80.20 and higher" on page 522\*](#)

For additional information related to these upgrade procedures, see [sk163814](#).

# Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Check Point server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- These instructions equally apply to:
  - Endpoint Security Management Server
  - Endpoint Policy Server
- For additional information related to this upgrade, see [sk163814](#).

**Important** - Before you upgrade an Endpoint Security Management Server or Endpoint Policy Server:



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server or Endpoint Policy Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Endpoint Security Management Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the server**

**Important** - See "[Management Server Migration Tool and Upgrade Tools](#)" on [page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools</a>" on <a href="#">page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia</a>" on <a href="#">page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. Upgrade the Endpoint Security Management Server or Endpoint Policy Server with CPUSE**

See "[Installing Software Packages on Gaia](#)" on [page 160](#) and follow the applicable action plan.

**3. Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on [page 89](#).

**4. Upgrade the dedicated Endpoint Policy Servers**

This step is part of the upgrade procedure of a Endpoint Security Management Server server. If you upgrade a dedicated Endpoint Policy Server, then skip this step.



**Important** - If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must upgrade these dedicated servers to the same version as the Endpoint Security Management Server.

Select the applicable upgrade option from these:

- For R80.20 and higher:

*"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher" on page 499*

- For R80.10 and lower:

*"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482*

## 5. Update the object version of the dedicated Endpoint Policy Servers



**Important** - If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must update the version of the corresponding objects in SmartConsole.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 6. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 7. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit Software Blade** is enabled on the R80.40 Endpoint Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 8. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <div style="border: 1px solid black; padding: 5px; width: fit-content;">cp_log_export reconf</div>
4	Restart the Log Exporter: <div style="border: 1px solid black; padding: 5px; width: fit-content;">cp_log_export restart</div>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter *Log Exporter*.

## 9. Test the functionality on the R80.40 Endpoint Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server. Make sure the management database and configuration were upgraded correctly.
2	Connect with SmartConsole to the R80.40 Endpoint Policy Server. Make sure the everything works correctly.

# Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Check Point server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- These instructions equally apply to:
  - Endpoint Security Management Server
  - Endpoint Policy Server
- For additional information related to this upgrade, see [sk163814](#).

**Important** - Before you upgrade an Endpoint Security Management Server or Endpoint Policy Server:



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server or Endpoint Policy Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Endpoint Security Management Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "*Management Server Migration Tool and Upgrade Tools*" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<i>Management Server Migration Tool and Upgrade Tools</i>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<i>Installing Software Packages on Gaia</i>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Endpoint Security Management Server or Endpoint Policy Server, run the**

## Pre-Upgrade Verifier and export the entire management database

Step	Instructions
1	Connect to the command line on the source Endpoint Server.
2	Log in to the Expert mode.
5	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre>cd \$FWDIR/scripts</pre>
3	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is</i> connected to the Internet, run:</li> <pre>./migrate_server verify -v R80.40</pre> <li>■ If this Endpoint Server <i>is not</i> connected to the Internet, run:</li> <pre>./migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</p>
4	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol>
4	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is</i> connected to the Internet, run:</li> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <li>■ If this Endpoint Server <i>is not</i> connected to the Internet, run:</li> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ You can also export the MSI packages with the "--include-uepm-msi-files" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>

### 3. Install a new R80.40 Endpoint Security Management Server or Endpoint Policy Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.

Step	Instructions
2	<p>Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia" on page 160</a> - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing an Endpoint Security Management Server" on page 77</a>.</li> <li>■ Follow "<a href="#">Installing an Endpoint Policy Server" on page 82</a>.</li> </ul> <p><b>Important</b> - These options are available:</p>  <ul style="list-style-type: none"> <li>■ The IP addresses of the source and target servers <b>can be the same</b>. If in the future it is necessary to have a different IP address on the R80.40 server, you can change it. For applicable procedures, see <a href="#">sk40993</a> and <a href="#">sk65451</a>. Note that you have to issue licenses for the new IP address.</li> <li>■ The IP addresses of the source and target servers <b>can be different</b>. Note that you have to issue licenses for the new IP address. You must install the new licenses only after you import the databases.</li> </ul>

#### 4. Get the required Upgrade Tools on the R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools" on page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools" on page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia" on page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.

## 5. On the target R80.40 Endpoint Security Management Server or Endpoint Policy Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Endpoint Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
4	<p>Transfer the exported databases from an external storage to the R80.40 Endpoint Server, to some directory.</p> <p> <b>Note</b> - Make sure to transfer the files in the binary mode.</p>
5	<p>Make sure the transferred files are not corrupted.</p> <p>Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Endpoint Server:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre>cd \$FWDIR/scripts/</pre>

Step	Instructions
7	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is not</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands).</li> <li>■ You can also import the MSI packages with the "--include-uepm-msi-files" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</li> </ul>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Install the new licenses



**Important** - This step applies only if the target R80.40 Endpoint Server has a different IP address than the source Endpoint Server.

Step	Instructions
1	Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.
2	Install the new licenses on the R80.40 Endpoint Server. You can do this either in the CLI with the "cplic put" command, or in the Gaia Portal.
3	Wait for a couple of minutes for the Endpoint Server to detect the new licenses. Alternatively, restart Check Point services: <pre>cpstop cpstart</pre>

## 8. Upgrade the dedicated Endpoint Policy Servers

This step is part of the upgrade procedure of a Endpoint Security Management Server server. If you upgrade a dedicated Endpoint Policy Server, then skip this step.



**Important** - If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must upgrade these dedicated servers to the same version as the Endpoint Security Management Server.

Select the applicable upgrade option from these:

- For R80.20 and higher:

*"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher" on page 499*

- For R80.10 and lower:

*"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482*

## 9. Update the object version of the dedicated Endpoint Policy Servers



**Important** - If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must update the version of the corresponding objects in SmartConsole.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 11. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Endpoint Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 12. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <code>cp_log_export reconf</code>
4	Restart the Log Exporter: <code>cp_log_export restart</code>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 13. Test the functionality on the R80.40 Endpoint Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server. Make sure the management database and configuration were upgraded correctly.
2	Connect with SmartConsole to the R80.40 Endpoint Policy Server. Make sure the everything works correctly.

# Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration

In a migration and upgrade scenario, you perform the procedure on the source Check Point server and the different target Check Point server.

## Notes:



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- These instructions equally apply to:
  - Endpoint Security Management Server
  - Endpoint Policy Server
- For additional information related to this upgrade, see [sk163814](#).

**Important** - Before you upgrade an Endpoint Security Management Server or Endpoint Policy Server:



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server or Endpoint Policy Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Endpoint Security Management Server is upgraded and runs, before you start the upgrade on other servers.

**Procedure:****1. Get the required Upgrade Tools on the source server**

**Important** - See "*Management Server Migration Tool and Upgrade Tools*" on page 182 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<i>Management Server Migration Tool and Upgrade Tools</i>" on page 182.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<i>Installing Software Packages on Gaia</i>" on page 160 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <code>ngm_upgrade_wrapper_993000222_1.tgz</code></p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

```
Timeout. Failed to retrieve Upgrade Tools package. To
download the package manually, refer to sk135172.
```

**2. On the current Endpoint Security Management Server or Endpoint Policy Server, run the**

## Pre-Upgrade Verifier and export the entire management database

Step	Instructions
1	Connect to the command line on the source Endpoint Server.
2	Log in to the Expert mode.
5	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre>cd \$FWDIR/scripts</pre>
3	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is</i> connected to the Internet, run:</li> <pre>./migrate_server verify -v R80.40</pre> <li>■ If this Endpoint Server <i>is not</i> connected to the Internet, run:</li> <pre>./migrate_server verify -v R80.40 -skip_upgrade_tools_check</pre> </ul> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</p>
4	<p>Read the Pre-Upgrade Verifier output.</p> <p>If it is necessary to fix errors:</p> <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol>
4	<p>Export the management database:</p> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is</i> connected to the Internet, run:</li> <pre>./migrate_server export -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <li>■ If this Endpoint Server <i>is not</i> connected to the Internet, run:</li> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ You can also export the MSI packages with the "--include-uepm-msi-files" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</li> </ul>
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>

### 3. Install a new R80.40 Endpoint Security Management Server or Endpoint Policy Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.

Step	Instructions
2	<p>Perform the clean install in one of these ways (do <b>not</b> perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia" on page 160</a> - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing an Endpoint Security Management Server" on page 77</a>.</li> <li>■ Follow "<a href="#">Installing an Endpoint Policy Server" on page 82</a>.</li> </ul> <p><b>Important</b> - These options are available:</p>  <ul style="list-style-type: none"> <li>■ The IP addresses of the source and target servers <b>can be the same</b>. If in the future it is necessary to have a different IP address on the R80.40 server, you can change it. For applicable procedures, see <a href="#">sk40993</a> and <a href="#">sk65451</a>. Note that you have to issue licenses for the new IP address.</li> <li>■ The IP addresses of the source and target servers <b>can be different</b>. Note that you have to issue licenses for the new IP address. You must install the new licenses only after you import the databases.</li> </ul>

#### 4. Get the required Upgrade Tools on the target R80.40 server



**Important** - See "[Management Server Migration Tool and Upgrade Tools" on page 182](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R80.40 Upgrade Tools from the <a href="#">sk135172</a>. (See "<a href="#">Management Server Migration Tool and Upgrade Tools" on page 182</a>.)</p> <p><b>Note</b> - This is a CPUSE Offline package.</p>
2	<p>Install the R80.40 Upgrade Tools with CPUSE. See "<a href="#">Installing Software Packages on Gaia" on page 160</a> and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed. Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p><b>Example</b></p> <p>Name of the downloaded package: <a href="#">ngm_upgrade_wrapper_993000222_1.tgz</a></p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R80.40 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>



**Note** - The command "migrate\_server" from these Upgrade Tools always tries to connect to Check Point Cloud over the Internet.

This is to make sure you always have the latest version of these Upgrade Tools installed.

If the connection to Check Point Cloud fails, this message appears:

Timeout. Failed to retrieve Upgrade Tools package. To download the package manually, refer to sk135172.

## 5. On the target R80.40 Endpoint Security Management Server or Endpoint Policy Server, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Endpoint Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre>cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
4	<p>Transfer the exported databases from an external storage to the R80.40 Endpoint Server, to some directory.</p> <p> <b>Note</b> - Make sure to transfer the files in the binary mode.</p>
5	<p>Make sure the transferred files are not corrupted.</p> <p>Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Endpoint Server:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre>cd \$FWDIR/scripts/</pre>

Step	Instructions
7	<p>Import the management database:</p> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <ul style="list-style-type: none"> <li>■ If this Endpoint Server <i>is not</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands).</li> <li>■ You can also import the MSI packages with the "--include-uepm-msi-files" option.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate_server</i>.</li> </ul>

## 6. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 7. Install the new licenses



**Important** - This step applies only if the target R80.40 Endpoint Server has a different IP address than the source Endpoint Server.

Step	Instructions
1	Issue licenses for the new IP address in your <a href="#">Check Point User Center</a> account.
2	Install the new licenses on the R80.40 Endpoint Server. You can do this either in the CLI with the "cplic put" command, or in the Gaia Portal.
3	Wait for a couple of minutes for the Endpoint Server to detect the new licenses. Alternatively, restart Check Point services: <pre>cpstop cpstart</pre>

## 8. Upgrade the dedicated Endpoint Policy Servers

This step is part of the upgrade procedure of a Endpoint Security Management Server server. If you upgrade a dedicated Endpoint Policy Server, then skip this step.



**Important** - If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must upgrade these dedicated servers to the same version as the Endpoint Security Management Server.

Select the applicable upgrade option from these:

- For R80.20 and higher:

[\*"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher" on page 499\*](#)

- For R80.10 and lower:

[\*"Upgrading a Dedicated Endpoint Policy Server from R80.10 and lower" on page 482\*](#)

## 9. Update the object version of the dedicated Endpoint Policy Servers



**Important** - If your Endpoint Security Management Server manages dedicated Endpoint Policy Servers, you must update the version of the corresponding objects in SmartConsole.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click <b>General Properties</b> .
5	In the <b>Platform</b> section > in the <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

## 10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 11. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Endpoint Server.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Endpoint Server.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 12. Reconfigure the Log Exporter

Step	Instructions
1	Connect to the command line on the server.
2	Log in to the Expert mode.
3	Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre>
4	Restart the Log Exporter: <pre>cp_log_export restart</pre>

For more information, see the [R80.40 Logging and Monitoring Administration Guide](#) > Chapter Log Exporter.

## 13. Test the functionality on the R80.40 Endpoint Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Endpoint Security Management Server. Make sure the management database and configuration were upgraded correctly.
2	Connect with SmartConsole to the R80.40 Endpoint Policy Server. Make sure the everything works correctly.

**14. Disconnect the old Endpoint Server from the network**

Disconnect the cables from the old Endpoint Server.

**15. Connect the new Endpoint Server to the network**

Connect the cables to the new Endpoint Server.

# Upgrading Endpoint Security Management Servers in Management High Availability from R80.20 and higher

**Notes:**



- This procedure is supported only for servers that run R80.20.M1, R80.20, R80.20.M2, or R80.30.
- For additional information related to this upgrade, see [sk163814](#).

**Important** - Before you upgrade an Endpoint Security Management Server:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to <b>Publish</b> the session.
4	You must close all GUI clients (SmartConsole applications) connected to the source Endpoint Security Management Server or Endpoint Policy Server.
5	Install the latest version of the CPUSE from <a href="#">sk92449</a> . <b>Note</b> - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
6	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
7	In Management High Availability, make sure the Primary Endpoint Security Management Server is upgraded and runs, before you start the upgrade on other servers.



**Important** - Before you can install Hotfixes on servers that work in Management High Availability, you must upgrade all these servers.

**Procedure:**

Step	Instructions
1	<p>Upgrade the <b>Primary</b> Endpoint Security Management Server with one of the supported methods.</p> <ul style="list-style-type: none"> <li>■ CPUSE See "<i>Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE</i>" on page 500</li> <li>■ Advanced Upgrade See "<i>Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade</i>" on page 505</li> <li>■ Migration See "<i>Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration</i>" on page 513</li> </ul>
2	<p>Upgrade the <b>Secondary</b> Endpoint Security Management Server with one of the supported methods.</p> <ul style="list-style-type: none"> <li>■ CPUSE See "<i>Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE</i>" on page 500</li> <li>■ Advanced Upgrade See "<i>Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade</i>" on page 505</li> <li>■ Migration See "<i>Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration</i>" on page 513</li> </ul>
3	<p>Get the R80.40 SmartConsole. See "<i>Installing SmartConsole</i>" on page 89.</p>
4	<p>Connect with SmartConsole to the R80.40 Primary Endpoint Security Management Server.</p>
5	<p>Update the object version of the Secondary Endpoint Security Management Server:</p> <ol style="list-style-type: none"> <li>a. From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>b. Open the Secondary Endpoint Security Management Server object.</li> <li>c. From the left tree, click <b>General Properties</b>.</li> <li>d. In the <b>Platform</b> section &gt; in the <b>Version</b> field, select <b>R80.40</b>.</li> <li>e. Click <b>OK</b>.</li> </ol>
6	<p>Make sure Secure Internal Communication (SIC) works correctly with the Secondary Security Management Server:</p> <ol style="list-style-type: none"> <li>a. From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li> <li>b. Open the Secondary Security Management Server object.</li> <li>c. On the <b>General Properties</b> page, click <b>Communication</b>.</li> <li>d. Click <b>Test SIC Status</b>. The SIC Status must show <b>Communicating</b>.</li> <li>e. Click <b>Close</b>.</li> <li>f. Click <b>OK</b>.</li> </ol>

Step	Instructions
7	<p>Install the management database:</p> <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Install database</b>.</li> <li>b. Select all objects.</li> <li>c. Click <b>Install</b>.</li> <li>d. Click <b>OK</b>.</li> </ol>
8	<p>Install the Event Policy.</p> <p> <b>Important</b> - This step applies only if the <b>SmartEvent Correlation Unit Software Blade</b> is enabled on the R80.40 Endpoint Security Management Server.</p> <ol style="list-style-type: none"> <li>a. In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b>.</li> <li>b. At the top, click <b>+</b> to open a new tab.</li> <li>c. In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b>.</li> </ol> <p>The Legacy SmartEvent client opens.</p> <ol style="list-style-type: none"> <li>d. In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b>.</li> <li>e. Confirm.</li> <li>f. Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded</li> <li>g. Click <b>Close</b>.</li> <li>h. Close the Legacy SmartEvent client.</li> </ol>
9	<p>Reconfigure the Log Exporter:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the server.</li> <li>b. Log in to the Expert mode.</li> <li>c. Reconfigure the Log Exporter: <pre>cp_log_export reconf</pre></li> <li>d. Restart the Log Exporter: <pre>cp_log_export restart</pre></li> </ol>
10	<p>For more information, see the <a href="#">R80.40 Logging and Monitoring Administration Guide</a> &gt; Chapter <i>Log Exporter</i></p> <p>Synchronize the Endpoint Security Management Servers:</p> <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Management High Availability</b>.</li> <li>b. In the <b>Peers</b> section, click <b>Actions &gt; Sync Peer</b>.</li> <li>c. The status must show <b>Successfully synced</b> for all peers.</li> </ol>

# Upgrade of Security Gateways and Clusters

This section provides instructions to upgrade Security Gateways and Clusters:

- "[Upgrading a Security Gateway or VSX Gateway](#)" on page 526
- "[Upgrading ClusterXL, VSX Cluster, or VRRP Cluster](#)" on page 538
- "[Full High Availability Cluster on Check Point Appliances](#)" on page 143

# Upgrading a Security Gateway or VSX Gateway

This section provides instructions to upgrade a Security Gateway or VSX Gateway:

- [\*"Upgrading a Security Gateway with CPUSE" on page 527\*](#)
- [\*"Upgrading a VSX Gateway with CPUSE" on page 531\*](#)

# Upgrading a Security Gateway with CPUSE

## Notes:



- In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Security Gateway.
- This upgrade method is supported only for Security Gateways that already run Gaia Operating System.

**Important - Before you upgrade a Security Gateway:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Upgrade the Management Server and Log Servers.
4	Upgrade the licenses on the Security Gateway, if needed. See " <a href="#">Working with Licenses</a> " on page 791.
4	<b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b> The upgrade process replaces all existing files with default files. If you have custom configurations on the Security Gateway, they are lost during the upgrade. As a result, different issues can occur in the upgraded Security Gateway.

**Procedure:**

- On the Security Gateway, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40**



**Important** - You must reboot the Security Gateway after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 from scratch	<p>Follow "<a href="#">Installing a Security Gateway</a>" on page 93 - only the step "Install the Security Gateway".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Security Gateway (prior to the upgrade).</p>

- In SmartConsole, establish SIC with the Security Gateway**



**Important** - This step is required only if you performed a Clean Install of R80.40 on this Security Gateway.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <b>Main Domain Management Server</b> that manages this Security Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Security Gateway object.
4	From the left tree, click <b>General Properties</b> .
5	Click the <b>Communication</b> button.
6	Click <b>Reset</b> .
7	In the <b>One-time password</b> field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Security Gateway.

Step	Instructions
8	In the <b>Confirm one-time password</b> field, enter the same Activation Key again.
9	Click <b>Initialize</b> .
10	The <b>Trust state</b> field must show <b>Trust established</b> .
11	Click <b>Close</b> to close the <b>Communication</b> window.
12	Click <b>OK</b> to close the <b>Security Gateway Properties</b> window.
13	Publish the SmartConsole session.

### 3. In SmartConsole, change the version of the Security Gateway object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Security Gateway object.
4	From the left tree, click the <b>General Properties</b> page.
5	In the <b>Platform</b> section > <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> .

### 4. In SmartConsole, install the Policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Install the Access Control Policy: <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>Click <b>Install</b>.</li> <li>The Access Control Policy must install successfully.</li> </ol>
4	Install the Threat Prevention Policy: <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Threat Prevention Policy.</li> <li>Click <b>Install</b>.</li> <li>The Threat Prevention Policy must install successfully.</li> </ol>

### 5. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .
3	Examine the logs from this Security Gateway to make sure it inspects the traffic as expected.

# Upgrading a VSX Gateway with CPUSE

## Notes:



- In a CPUSE upgrade scenario, you perform the upgrade procedure on the same VSX Gateway.
- This upgrade method is supported only for VSX Gateways that already run Gaia Operating System.

**Important - Before you upgrade a VSX Gateway:**



Step	Instructions
1	<p>Back up your current configuration (see "<a href="#">Backing Up and Restoring</a>" on page 27).</p> <p><b>Important - Back up both the Management Server and the VSX Gateway. Follow <a href="#">sk100395</a>.</b></p>
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	Upgrade the Management Server and Log Servers.
4	<p>Upgrade the licenses on the VSX Gateway, if needed. See "<a href="#">Working with Licenses</a>" on page 791.</p> <p><b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b> The upgrade process replaces all existing files with default files. If you have custom configurations on the VSX Gateway, they are lost during the upgrade. As a result, different issues can occur in the upgraded VSX Gateway.</p>

These upgrade scenarios are available:

- Upgrading the VSX Gateway with CPUSE to R80.40
- Clean Install of the R80.40 VSX Gateway

## Upgrading the VSX Gateway with CPUSE to R80.40

1. On the Management Server, upgrade the configuration of the VSX Gateway object to R80.40

Step	Instructions
1	Connect to the command line on the Security Management Server or Multi-Domain Server that manages this VSX Gateway.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, go to the context of the <i>Main</i> Domain Management Server that manages this VSX Gateway object: <pre>mdsenv &lt;IP Address or Name of Main Domain Management Server&gt;</pre>
4	Upgrade the configuration of the VSX Gateway object to R80.40: <pre>vsx_util upgrade</pre> <p>This command is interactive.</p> <p>Enter these details to log in to the management database:</p> <ul style="list-style-type: none"> <li>■ IP address of the Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Gateway</li> <li>■ Management Server administrator's username</li> <li>■ Management Server administrator's password</li> </ul> <p>Select your VSX Gateway.</p> <p>Select <b>R80.40</b>.</p> <p>For auditing purposes, save the <code>vsx_util</code> log file:</p> <ul style="list-style-type: none"> <li>■ On a Security Management Server:  <pre>/opt/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> </li> <li>■ On a Multi-Domain Server:  <pre>/opt/CPmds-R80.40/customers/&lt;Name_of_Domain&gt;/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> </li> </ul>
5	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Gateway.
6	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
7	Open the VSX Gateway object.
8	From the left tree, click the <b>General Properties</b> page.
9	Make sure in the <b>Platform</b> section, the <b>Version</b> field shows <b>R80.40</b> .

Step	Instructions
10	<p>Click <b>Cancel</b> (do not click <b>OK</b>).</p>  <p><b>Note</b> - If you click <b>OK</b>, the Management Server pushes the VSX configuration to the VSX Gateway. Because the VSX Gateway is not upgraded yet, this operation would fail.</p>

## 2. Upgrade the VSX Gateway with CPUSE

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

## 3. In SmartConsole, install the policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Install the default policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the default policy for this VSX Gateway object. This policy is called:</li> </ol> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <i>&lt;Name of VSX Gateway object&gt;_VSX</i> </div> <ol style="list-style-type: none"> <li>Click <b>Install</b>.</li> </ol>
4	<p>Install the Threat Prevention Policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Threat Prevention Policy for this VSX Gateway object.</li> <li>Click <b>Install</b>.</li> </ol>

## 4. Test the functionality

Step	Instructions
1	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the VSX Gateway.</li> <li>Log in to the Expert mode.</li> <li>Run:</li> </ol> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <code>vsx stat -v</code> </div>
2	Connect with SmartConsole to the R80.40 Security Management Server or each <i>Target Domain Management Server</i> that manages the Virtual Systems on this VSX Gateway.
3	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .

Step	Instructions
4	Examine the logs from the Virtual Systems on this VSX Gateway to make sure they inspect the traffic as expected.

## Clean Install of the R80.40 VSX Gateway

1. On the Management Server, upgrade the configuration of the VSX Gateway object to R80.40

Step	Instructions
1	Connect to the command line on the Security Management Server or Multi-Domain Server that manages this VSX Gateway.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, go to the context of the <i>Main</i> Domain Management Server that manages this VSX Gateway object: <pre>mdsenv &lt;IP Address or Name of Main Domain Management Server&gt;</pre>
4	Upgrade the configuration of the VSX Gateway object to R80.40: <pre>vsx_util upgrade</pre> <p>This command is interactive.</p> <p>Enter these details to log in to the management database:</p> <ul style="list-style-type: none"> <li>■ IP address of the Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Gateway</li> <li>■ Management Server administrator's username</li> <li>■ Management Server administrator's password</li> </ul> <p>Select your VSX Gateway.</p> <p>Select <b>R80.40</b>.</p> <p>For auditing purposes, save the <code>vsx_util</code> log file:</p> <ul style="list-style-type: none"> <li>■ On a Security Management Server:  <pre>/opt/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> </li> <li>■ On a Multi-Domain Server:  <pre>/opt/CPmds-R80.40/customers/&lt;Name_of_Domain&gt;/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> </li> </ul>
5	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Gateway.
6	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
7	Open the VSX Gateway object.
8	From the left tree, click the <b>General Properties</b> page.
9	Make sure in the <b>Platform</b> section, the <b>Version</b> field shows <b>R80.40</b> .

Step	Instructions
10	<p>Click <b>Cancel</b> (do not click <b>OK</b>).</p>  <p><b>Note</b> - If you click <b>OK</b>, the Management Server pushes the VSX configuration to the VSX Gateway. Because the VSX Gateway is not upgraded yet, this operation would fail.</p>

## 2. On the VSX Gateway, perform a Clean Install of R80.40



**Important** - You must reboot the VSX Gateway after the upgrade or clean install.

Installation Method	Instructions
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation. In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 from scratch	<p>Follow "<a href="#">Installing a VSX Gateway</a>" on page 99 - only the step "<i>Install the VSX Gateway</i>".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Gateway (prior to the upgrade).</p>

## 3. Reconfigure the VSX Gateway

Step	Instructions
1	<p>Configure the required settings on the VSX Gateway.</p> <p>For more information, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>VSX Commands</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p>
2	Connect to the command line on the R80.40 Security Management Server or Multi-Domain Server that manages this VSX Gateway.
3	Log in to the Expert mode.
4	<p>On Multi-Domain Server, go to the context of the <i>Main Domain Management Server</i> that manages this VSX Gateway:</p> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;"> <pre>mdsenv &lt;IP Address or Name of Main Domain Management Server&gt;</pre> </div>

Step	Instructions
5	<p>Restore the VSX configuration:</p> <pre data-bbox="473 271 822 305">vsx_util reconfigure</pre> <p>Follow the instructions on the screen.</p> <p> <b>Important</b> - Enter the same Activation Key you entered during the First Time Configuration Wizard of the VSX Gateway.</p>
6	<p>Configure the required settings on the VSX Gateway:</p> <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul>

#### 4. Test the functionality

Step	Instructions
1	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="557 1051 747 1084">vsx stat -v</pre>
2	<p>Connect with SmartConsole to the R80.40 Security Management Server or each <i>Target Domain</i> Management Server that manages the Virtual Systems on this VSX Gateway.</p>
3	<p>From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b>.</p>
4	<p>Examine the logs from the Virtual Systems on this VSX Gateway to make sure they inspect the traffic as expected.</p>

For more information, see the:

- [R80.40 VSX Administration Guide](#).
- [R80.40 CLI Reference Guide](#).

# Upgrading ClusterXL, VSX Cluster, or VRRP Cluster

This section provides instructions to upgrade a cluster:

- [\*"Planning a Cluster Upgrade" on page 539\*](#)
- [\*"Minimal Effort Upgrade" on page 544\*](#)
- [\*"Zero Downtime Upgrade" on page 555\*](#)
- [\*"Multi-Version Cluster \(MVC\) Upgrade" on page 576\*](#)

These instructions equally apply to these clusters:

- ClusterXL
- VSX Cluster
- VRRP Cluster

These instructions equally apply to these software packages:

- Upgrade
- Clean Install
- Hotfixes (does not require the change of the version in the cluster object)

# Planning a Cluster Upgrade

**Important - Before you upgrade Cluster Members:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Upgrade the Management Server and Log Servers.
4	Upgrade the licenses on the Cluster Members, if needed. See " <a href="#">Working with Licenses" on page 791</a> .
5	If you upgrade a VSX Cluster, then on the Management Server you must upgrade the configuration of the VSX Cluster object to R80.40.
6	<b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b> The upgrade process replaces all existing files with default files. If you have custom configurations on the Cluster Members, they are lost during the upgrade. As a result, different issues can occur in the upgraded cluster. Cluster Members can stop detecting each other, Cluster Members can move to undesired state, and traffic can be dropped.
7	Make sure the configuration and the values of the required kernel parameters are the same on all Cluster Members. Log in to the Expert mode on <i>each</i> Cluster Member and run the applicable commands (see below).



**Note** - For more information, see [sk25977](#).

## Applicable commands and required kernel parameters

Version	Mode	Applicable Command and Parameters
R80.10 and higher	Cluster Members	<pre>cphaprof mmagic</pre> <p>Examine the value in the "MAC magic" field. Examine the value in the "MAC forward magic" field.</p>
	VSX Cluster Members	<pre>fw ctl get int fwha_add_vsid_to_ccp_mac grep fwha_add_vsid_to_ccp_mac \$FWDIR/boot/modules/fw kern.conf</pre> <p>Examine the value of the kernel parameter "fwha_add_vsid_to_ccp_mac".</p>
R77.30	Cluster Members	<pre>cphaconf cluster_id get</pre> <p>Examine the value of the "cluster_id".</p>
	VSX Cluster Members	<pre>fw ctl get int fwha_add_vsid_to_ccp_mac grep fwha_add_vsid_to_ccp_mac \$FWDIR/boot/modules/fw kern.conf</pre> <p>Examine the value of the kernel parameter "fwha_add_vsid_to_ccp_mac".</p>
R75.40 - R77.20	Cluster Members, VSX Cluster Members	<pre>fw ctl get int fwha_mac_magic fw ctl get int fwha_mac_forward_magic</pre> <p>Examine the value of the kernel parameter "fwha_mac_magic". Examine the value of the kernel parameter "fwha_mac_forward_magic".</p>

## Available upgrade methods:

Because the upgrade process on Cluster Members stops all Check Point services, it disrupts the cluster's ability to inspect and synchronize the connections that pass through the cluster.

The table below describes the available upgrade methods.

Upgrade Method	Instructions	Maintenance Window (downtime)	Limitations
<a href="#">"Multi-Version Cluster (MVC) Upgrade" on page 576</a>	<p>Select this method, if connectivity is of utmost concern.            Connection failover is guaranteed - no connections are dropped.</p> <p><b>Connections that were initiated before the upgrade are synchronized with the upgraded Security Gateways and cluster members, so that no connections are dropped.</b></p> <p>You can select this method, if you upgrade a ClusterXL or a VSX Cluster.            You can select this method, if you upgrade a 3rd party cluster (VRRP on Gaia).</p>	<p>This upgrade method does not require a downtime window.  <b>Duration of this upgrade is short.</b></p>	<p>This upgrade method supports only specific upgrade paths.            Many types of connections do not survive after failover to upgraded Cluster Member.</p> <p>See:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Supported Versions in Multi-Version Cluster" on page 577</a></li> <li>■ <a href="#">"Multi-Version Cluster Limitations" on page 578.</a></li> </ul>
<a href="#">"Minimal Effort Upgrade" on page 544 (Simple Upgrade)</a>	<p>Select this method, if you have a period of time, during which network downtime is allowed.</p> <p>This method is the simplest, because it lets you upgrade each Cluster Member as an independent Security Gateway.</p> <p><b>All connections that were initiated before the upgrade, are dropped during the upgrade.</b></p> <p>You can select this method, if you upgrade a ClusterXL or a VSX Cluster.            You can select this method, if you upgrade a 3rd party cluster (VRRP on Gaia).</p>	<p>This upgrade method requires a substantial downtime window.  <b>Duration of this upgrade is as long as it takes to upgrade all Cluster Members.</b></p>	None

Upgrade Method	Instructions	Maintenance Window (downtime)	Limitations
<a href="#">"Zero Downtime Upgrade" on page 555</a>	<p>Select this method, if you cannot have any network downtime and need to complete the upgrade quickly, with a minimal number of dropped connections.</p> <p>During this type of upgrade, there is always at least one Active Cluster Member in cluster that handles traffic.</p> <p><b>All connections that were initiated through a Cluster Member that runs the old version, are dropped when you upgrade that Cluster Member to a new version,</b> because Cluster Members that run different Check Point software versions, <b>cannot synchronize connections.</b></p> <p>Network connectivity, however, remains available during the upgrade, and connections initiated through an upgraded cluster member are not dropped.</p> <p>You can select this method, if you upgrade a ClusterXL or a VSX Cluster.</p> <p>You can select this method, if you upgrade a 3rd party cluster (VRRP on Gaia).</p>	<p>This upgrade method requires a relatively short downtime window to drop old connections.</p> <p><b>Duration of this upgrade is relatively short.</b></p>	<p>This upgrade method does not support Dynamic Routing connections.</p>

## Cluster state "Ready" during a cluster upgrade



**Note** - This applies only when the Multi-Version Cluster (MVC) Mechanism is disabled (see "[Multi-Version Cluster \(MVC\) Upgrade](#)" on page 576).

When Cluster Members of different versions are on the same network, Cluster Members of the new (upgraded) version remain in the state **Ready**, and Cluster Members of the previous version remain in state **Active Attention**.

Cluster Members in the state **Ready** do not process traffic and do not synchronize with other Cluster Members.

To prevent Cluster Members from being in the state "Ready":

Option	Instructions
1	<p>Perform these steps:</p> <ol style="list-style-type: none"><li>Connect over the console to the Cluster Member.</li><li>Physically disconnect the Cluster Member from the network (disconnect all cables).</li></ol>
2	<p>Perform these steps:</p> <ol style="list-style-type: none"><li>Connect over the console to the Cluster Member.</li><li>Log in to Gaia Clish..</li><li>Shut down all interfaces: <pre>set interface &lt;Name of Interface&gt; state off</pre></li></ol>

For more information, see [sk42096](#).

# Minimal Effort Upgrade

This section provides instructions for Minimal Effort Upgrade (Simple Upgrade):

- [\*"Minimal Effort Upgrade of a Security Gateway Cluster" on page 545\*](#)
- [\*"Minimal Effort Upgrade of a VSX Cluster" on page 549\*](#)



**Important** - You can use this upgrade method for all supported versions as described in the [R80.40 Release Notes](#).

## Minimal Effort Upgrade of a Security Gateway Cluster

**Important - Before you upgrade a Cluster:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Upgrade the Management Server and Log Servers.
4	See " <a href="#">Planning a Cluster Upgrade" on page 539</a> .
5	Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.

**Procedure:**

1. **On each Cluster Member, Upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40**



**Important -** You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia" on page 160</a>. Follow the applicable action plan for the local or central installation. In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia" on page 160</a>. Follow the applicable action plan for the local or central installation. In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p> <b>Important -</b> In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p>

Installation Method	Instructions
Clean Install of R80.40 from scratch	<p><b>Installing a Cluster Member</b></p> <p>Follow "<a href="#">Installing a ClusterXL Cluster</a> on page 105" - only the step "Install the Cluster Members".</p>  <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p><b>Installing a VRRP Cluster Member</b></p> <p>Follow "<a href="#">Installing a VRRP Cluster</a> on page 129" - only the step "Install the VRRP Cluster Members".</p>  <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p><b>Installing a VSX Cluster Member</b></p> <p>Follow "<a href="#">Installing a VSX Cluster</a> on page 123" - only the step "Install the VSX Cluster Members".</p>  <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p>

## 2. In SmartConsole, change the version of the cluster object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Cluster object.
4	From the left tree, click the <b>General Properties</b> page.
5	In the <b>Platform</b> section > <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> to close the <b>Gateway Cluster Properties</b> window.

## 3. In SmartConsole, install the Access Control Policy and Threat Prevention Policy on the Cluster object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	<p>Install the Access Control Policy:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>In the <b>Install Mode</b> section, select these two options: <ul style="list-style-type: none"> <li>■ <b>Install on each selected gateway independently</b></li> <li>■ <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b></li> </ul> </li> <li>Click <b>Install</b>.</li> <li>The Access Control Policy must install successfully on all the Cluster Members.</li> </ol>
4	<p>Install the Threat Prevention Policy:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Threat Prevention Policy.</li> <li>Click <b>Install</b>.</li> <li>The Threat Prevention Policy must install successfully on all the Cluster Members.</li> </ol>

#### 4. On each Cluster Member, examine the cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:  <pre>show cluster state</pre> </li> <li>■ In the Expert mode, run:  <pre>cphaprof state</pre> </li> </ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ All Cluster Members must show the same information about the states of all Cluster Members.</li> <li>■ In the High Availability mode, one Cluster Member must be in the <b>Active</b> state, and all other Cluster Members must be in <b>Standby</b> state.</li> <li>■ In the Load Sharing modes, all Cluster Members must be in the <b>Active</b> state.</li> </ul>

#### 5. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .

Step	Instructions
3	Examine the logs from this Cluster to make sure it inspects the traffic as expected.

**For more information:**

See the [\*R80.40 ClusterXL Administration Guide\*](#).

## Minimal Effort Upgrade of a VSX Cluster

**Important - Before you upgrade a VSX Cluster:**

Step	Instructions
1	<p>Back up your current configuration (see "<a href="#">Backing Up and Restoring" on page 27</a>).</p> <p><b>Important -</b> Back up both the Management Server and the VSX Cluster Members. Follow <a href="#">sk100395</a>.</p>
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Upgrade the Management Server and Log Servers.
4	See " <a href="#">Planning a Cluster Upgrade" on page 539</a> .
5	<b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b>

### Procedure:

1. **On the Management Server, upgrade the configuration of the VSX Cluster object to R80.40**

Step	Instructions
1	Connect to the command line on the Security Management Server or Multi-Domain Server that manages this VSX Cluster.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, go to the context of the <i>Main Domain Management Server</i> that manages this VSX Cluster object: <pre>mdserv &lt;IP Address or Name of Main Domain Management Server&gt;</pre>
4	<p>Upgrade the configuration of the VSX Cluster object to R80.40:  <pre>vsx_util upgrade</pre> </p> <p>This command is interactive.</p> <p>Enter these details to log in to the management database:</p> <ul style="list-style-type: none"> <li>■ IP address of the Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Cluster</li> <li>■ Management Server administrator's username</li> <li>■ Management Server administrator's password</li> </ul> <p>Select your VSX Cluster.</p>

Step	Instructions
	<p>Select <b>R80.40</b>.</p> <p>For auditing purposes, save the <code>vsx_util</code> log file:</p> <ul style="list-style-type: none"> <li>■ On a Security Management Server:</li> </ul> <pre>/opt/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> <ul style="list-style-type: none"> <li>■ On a Multi-Domain Server:</li> </ul> <pre>/opt/CPmds-R80.40/customers/&lt;Name_of_Domain&gt;/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre>
5	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
6	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
7	Open the VSX Cluster object.
8	From the left tree, click the <b>General Properties</b> page.
9	Make sure in the <b>Platform</b> section, the <b>Version</b> field shows <b>R80.40</b> .
10	<p>Click <b>Cancel</b> (do not click <b>OK</b>).</p>  <p><b>Note</b> - If you click <b>OK</b>, the Management Server pushes the VSX configuration to the VSX Cluster. Because the VSX Cluster is not upgraded yet, this operation would fail.</p>

## 2. On each VSX Cluster Member, Upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>

Installation Method	Instructions
Clean Install of R80.40 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160. Follow the applicable action plan for the local or central installation. In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</li> </ol> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>
Clean Install of R80.40 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Follow "<a href="#">Installing a VSX Cluster</a>" on page 123 - only the step "Install the VSX Cluster Members".</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</li> </ol> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

### 3. In SmartConsole, install the policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Install the default policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the default policy for this VSX Cluster object. This policy is called:  <div style="border: 1px solid black; padding: 2px; display: inline-block;">&lt;Name of VSX Cluster object&gt;_VSX</div> </li> <li>In the <b>Install Mode</b> section, select these two options: <ul style="list-style-type: none"> <li>■ <b>Install on each selected gateway independently</b></li> <li>■ <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b></li> </ul> </li> <li>Click <b>Install</b>.</li> <li>The default policy install successfully on all the VSX Cluster Members.</li> </ol>
4	<p>Install the Threat Prevention Policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Threat Prevention Policy for this VSX Cluster object.</li> <li>Click <b>Install</b>.</li> <li>The Threat Prevention Policy must install successfully on all the VSX Cluster Members.</li> </ol>

#### 4. On each VSX Cluster Member, examine the VSX configuration and cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	<p>Examine the VSX configuration:</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">vsx stat -v</div> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>

Step	Instructions
4	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> </ul> <pre data-bbox="520 316 859 384">set virtual-system 0 show cluster state</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode, run:</li> </ul> <pre data-bbox="520 451 759 518">vsenv 0 cphaprof state</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members.</li> <li>■ In the High Availability mode, one VSX Cluster Member must be in the <b>Active</b> state, and all other VSX Cluster Members must be in <b>Standby</b> state.</li> <li>■ In the Virtual System Load Sharing mode, all VSX Cluster Members must be in the <b>Active</b> state.</li> <li>■ All Virtual Systems must show the same information about the states of all Virtual Systems.</li> </ul>
5	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> </ul> <pre data-bbox="520 1136 1113 1203">set virtual-system 0 show cluster members interfaces all</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode, run:</li> </ul> <pre data-bbox="520 1271 759 1338">vsenv 0 cphaprof -a if</pre>

## 5. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or each <i>Target</i> Domain Management Server that manages the Virtual Systems on this VSX Cluster.
2	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .
3	Examine the logs from the Virtual Systems on this VSX Cluster to make sure they inspect the traffic as expected.

For more information, see the:

- [\*R80.40 VSX Administration Guide\*](#).
- [\*R80.40 ClusterXL Administration Guide\*](#).

# Zero Downtime Upgrade

This section provides instructions for Zero Downtime Upgrade:

- [\*"Zero Downtime Upgrade of a Security Gateway Cluster" on page 556\*](#)
- [\*"Zero Downtime Upgrade of a VSX Cluster" on page 564\*](#)



**Important** - You can use this upgrade method for all supported versions as described in the [R80.40 Release Notes](#).

# Zero Downtime Upgrade of a Security Gateway Cluster

**Important - Before you upgrade a Cluster:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Upgrade the Management Server and Log Servers.
4	See " <a href="#">Planning a Cluster Upgrade" on page 539</a> .
5	<b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b>

The procedure below is based on an example cluster with three Cluster Members M1, M2 and M3.

However, you can use it for clusters that consist of two or more Cluster Members.

## Procedure:

### 1. On each Cluster Member, change the CCP mode to Broadcast



**Important -** This step does **not** apply to R80.30 with Linux kernel 3.10 (run the "uname -r" command).



**Best Practice -** To avoid possible problems with switches around the cluster during the upgrade, we recommend to change the Cluster Control Protocol (CCP) mode to Broadcast.

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Log in to the Expert mode.
3	Change the CCP mode to Broadcast: <pre>cphaconf set_ccp broadcast</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ This change does not require a reboot.</li> <li>■ This change applies immediately and survives reboot.</li> </ul>
4	Make sure the CCP mode is set to Broadcast: <pre>cphaprof -a if</pre>

### 2. On the Cluster Member M2, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p>
Clean Install of R80.40 from scratch	<p><b>Installing a Cluster Member</b></p> <p>Follow "<a href="#">Installing a ClusterXL Cluster</a>" on page 105 - only the step "Install the Cluster Members".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p><b>Installing a VRRP Cluster Member</b></p> <p>Follow "<a href="#">Installing a VRRP Cluster</a>" on page 129 - only the step "Install the VRRP Cluster Members".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p><b>Installing a VSX Cluster Member</b></p> <p>Follow "<a href="#">Installing a VSX Cluster</a>" on page 123 - only the step "Install the VSX Cluster Members".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p>

3. On the Cluster Member M3, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p>
Clean Install of R80.40 from scratch	<p><b>Installing a Cluster Member</b></p> <p>Follow "<a href="#">Installing a ClusterXL Cluster</a>" on page 105 - only the step "<i>Install the Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p><b>Installing a VRRP Cluster Member</b></p> <p>Follow "<a href="#">Installing a VRRP Cluster</a>" on page 129 - only the step "<i>Install the VRRP Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p><b>Installing a VSX Cluster Member</b></p> <p>Follow "<a href="#">Installing a VSX Cluster</a>" on page 123 - only the step "<i>Install the VSX Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p>

#### 4. In SmartConsole, change the version of the cluster object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Cluster object.
4	From the left tree, click the <b>General Properties</b> page.

Step	Instructions
5	In the <b>Platform</b> section > <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> to close the <b>Gateway Cluster Properties</b> window.

#### 5. In SmartConsole, install the Access Control Policy

Step	Instructions
1	Click <b>Install Policy</b> .
2	In the <b>Install Policy</b> window: <ol style="list-style-type: none"> <li>In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>In the <b>Install Mode</b> section, configure these two options:               <ul style="list-style-type: none"> <li>■ Select <b>Install on each selected gateway independently</b>.</li> <li>■ Clear <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b>.</li> </ul> </li> <li>Click <b>Install</b>.</li> </ol>
3	The Access Control Policy installation: <ul style="list-style-type: none"> <li>■ Succeeds on the <i>upgraded</i> Cluster Members <b>M2</b> and <b>M3</b>.</li> <li>■ Fails on the <i>old</i> Cluster Member <b>M1</b> with a warning. <b>Ignore this warning</b>.</li> </ul>

#### 6. On each Cluster Member, examine the cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish (R80.20 and higher), run:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">show cluster state</div> </li> <li>■ In the Expert mode, run:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">cphaprof state</div> </li> </ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ The cluster states of the upgraded Cluster Members <b>M2</b> and <b>M3</b> are <b>Ready</b>.</li> <li>■ The cluster state of the old Cluster Member <b>M1</b> is:               <ul style="list-style-type: none"> <li>• In R80.20 and higher - <b>Active (!)</b>.</li> <li>• In R80.10 and lower - <b>Active Attention</b>.</li> </ul> </li> </ul>

#### 7. On the old Cluster Member M1, stop all Check Point services

Step	Instructions
1	Connect to the command line on the Cluster Member <b>M1</b> .
2	<p>Stop all Check Point services:</p> <pre>cpstop</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ This forces a controlled cluster failover from the old Cluster Member <b>M1</b> to one of the upgraded Cluster Members.</li> <li>■ At this moment, all connections that were initiated through the old Cluster Member <b>M1</b> are dropped (because Cluster Members with different software versions cannot synchronize).</li> </ul>

#### 8. On each Cluster Member, examine the cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> </ul> <pre>show cluster state</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode, run:</li> </ul> <pre>cphaprof state</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ In the High Availability mode, one of the upgraded Cluster Members (<b>M2</b> or <b>M3</b>) changes its cluster state to <b>Active</b>. The other upgraded Cluster Member (<b>M2</b> or <b>M3</b>) changes its cluster state to <b>Standby</b>.</li> <li>■ In the Load Sharing modes, all Cluster Members must be in the <b>Active</b> state.</li> </ul>

#### 9. On the old Cluster Member M1, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p>
Clean Install of R80.40 from scratch	<p><b>Installing a Cluster Member</b></p> <p>Follow "<a href="#">Installing a ClusterXL Cluster</a>" on page 105 - only the step "<i>Install the Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p><b>Installing a VRRP Cluster Member</b></p> <p>Follow "<a href="#">Installing a VRRP Cluster</a>" on page 129 - only the step "<i>Install the VRRP Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p><b>Installing a VSX Cluster Member</b></p> <p>Follow "<a href="#">Installing a VSX Cluster</a>" on page 123 - only the step "<i>Install the VSX Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p>

#### 10. In SmartConsole, establish SIC with the Cluster Member M1



**Important** - This step is required only if you performed a Clean Install of R80.40 on this Cluster Member M1.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main Domain Management Server</i> that manages this Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	Open the cluster object.
4	From the left tree, click <b>Cluster Members</b> .
5	Select the object of the Cluster Member M1.
6	Click <b>Edit</b> .
7	On the <b>General</b> tab, click the <b>Communication</b> button.
8	Click <b>Reset</b> .
9	In the <b>One-time password</b> field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the <b>Confirm one-time password</b> field, enter the same Activation Key again.
11	Click <b>Initialize</b> .
12	The <b>Trust state</b> field must show <b>Trust established</b> .
13	Click <b>Close</b> to close the <b>Communication</b> window.
14	Click <b>OK</b> to close the <b>Cluster Member Properties</b> window.

11. In SmartConsole, install the Access Control Policy and Threat Prevention Policy on the Cluster object

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Install the Access Control Policy:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>In the <b>Install Mode</b> section, select these two options:           <ul style="list-style-type: none"> <li>■ <b>Install on each selected gateway independently</b></li> <li>■ <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b></li> </ul> </li> <li>Click <b>Install</b>.</li> <li>The Access Control Policy must install successfully on all the Cluster Members.</li> </ol>

Step	Instructions
4	<p>Install the Threat Prevention Policy:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Threat Prevention Policy.</li> <li>Click <b>Install</b>.</li> <li>The Threat Prevention Policy must install successfully on all the Cluster Members.</li> </ol>

## 12. On each Cluster Member, examine the cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">show cluster state</div> <li>■ In the Expert mode, run:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">cphaprof state</div> </ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ All Cluster Members must show the same information about the states of all Cluster Members.</li> <li>■ In the High Availability mode, one Cluster Member must be in the <b>Active</b> state, and all other Cluster Members must be in <b>Standby</b> state.</li> <li>■ In the Load Sharing modes, all Cluster Members must be in the <b>Active</b> state.</li> </ul>

## 13. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .
3	Examine the logs from this Cluster to make sure it inspects the traffic as expected.

### For more information:

See the [R80.40 ClusterXL Administration Guide](#).

## Zero Downtime Upgrade of a VSX Cluster

**Important - Before you upgrade a VSX Cluster:**

Step	Instructions
1	<p>Back up your current configuration (see "<a href="#">Backing Up and Restoring" on page 27</a>).</p> <p><b>Important -</b> Back up both the Management Server and the VSX Cluster Members. Follow <a href="#">sk100395</a>.</p>
2	See the " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Upgrade the Management Server and Log Servers.
4	See " <a href="#">Planning a Cluster Upgrade" on page 539</a> .
5	<b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b>

The procedure below describes an example VSX Cluster with three VSX Cluster Members M1, M2 and M3. However, you can use it for clusters that consist of two or more Cluster Members.

### Procedure:

1. **On the Management Server, upgrade the configuration of the VSX Cluster object to R80.40**

Step	Instructions
1	Connect to the command line on the Security Management Server or Multi-Domain Server that manages this VSX Cluster.
2	Log in to the Expert mode.
3	On a Multi-Domain Server, go to the context of the <i>Main Domain Management Server</i> that manages this VSX Cluster object: <pre>mdsenv &lt;IP Address or Name of Main Domain Management Server&gt;</pre>
4	<p>Upgrade the configuration of the VSX Cluster object to R80.40:  <pre>vsx_util upgrade</pre> </p> <p>This command is interactive.</p> <p>Enter these details to log in to the management database:</p> <ul style="list-style-type: none"> <li>■ IP address of the Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Cluster</li> <li>■ Management Server administrator's username</li> <li>■ Management Server administrator's password</li> </ul>

Step	Instructions
	Select your VSX Cluster.
	Select <b>R80.40</b> .
	<p>For auditing purposes, save the <code>vsx_util</code> log file:</p> <ul style="list-style-type: none"> <li>■ On a Security Management Server:</li> </ul> <pre>/opt/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> <ul style="list-style-type: none"> <li>■ On a Multi-Domain Server:</li> </ul> <pre>/opt/CPmds-R80.40/customers/&lt;Name_of_Domain&gt;/CPsuite-R80.40/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre>
5	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
6	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
7	Open the VSX Cluster object.
8	From the left tree, click the <b>General Properties</b> page.
9	Make sure in the <b>Platform</b> section, the <b>Version</b> field shows <b>R80.40</b> .
10	Click <b>Cancel</b> (do not click <b>OK</b> ).  <p><b>Note</b> - If you click <b>OK</b>, the Management Server pushes the VSX configuration to the VSX Cluster. Because the VSX Cluster is not upgraded yet, this operation would fail.</p>

## 2. On each VSX Cluster Member, change the CCP mode to Broadcast



**Important** - This step does **not** apply to R80.30 with Linux kernel 3.10 (run the "uname -r" command).



**Best Practice** - To avoid possible problems with switches around the cluster during the upgrade, we recommend to change the Cluster Control Protocol (CCP) mode to Broadcast.

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.

Step	Instructions
3	<p>Change the CCP mode to Broadcast:</p> <pre>cphaconf set_ccp broadcast</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ This change does not require a reboot.</li> <li>■ This change applies immediately and survives reboot.</li> </ul>
4	<p>Make sure the CCP mode is set to Broadcast:</p> <pre>cphaprof -a if</pre>

### 3. On the VSX Cluster Member M2, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</li> </ol> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p><b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

Installation Method	Instructions
Clean Install of R80.40 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Follow "<a href="#">Installing a VSX Cluster</a> on page 123" - only the step "Install the VSX Cluster Members".</li> </ol> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p>  <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p><b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p>  <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

4. **On the VSX Cluster Member M3, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40**



**Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>.</p> <p>See <a href="#">sk92449</a> for detailed steps.</p>

Installation Method	Instructions
Clean Install of R80.40 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160. Follow the applicable action plan for the local or central installation. In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</li> </ol> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>
Clean Install of R80.40 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Follow "<a href="#">Installing a VSX Cluster</a>" on page 123 - only the step "Install the VSX Cluster Members".</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</li> </ol> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

## 5. In SmartConsole, install the Access Control Policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Click <b>Install Policy</b> .
4	In the <b>Install Policy</b> window: <ol style="list-style-type: none"> <li>In the <b>Policy</b> field, select the default policy for this VSX Cluster object. This policy is called:  <b>&lt;Name of VSX Cluster object&gt;_VSX</b></li> <li>In the <b>Install Mode</b> section, configure these two options:               <ul style="list-style-type: none"> <li>■ Select <b>Install on each selected gateway independently</b>.</li> <li>■ Clear <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b>.</li> </ul> </li> <li>Click <b>Install</b>.</li> </ol>
5	The policy installation: <ul style="list-style-type: none"> <li>■ Succeeds on the <i>upgraded</i> VSX Cluster Members <b>M2</b> and <b>M3</b>.</li> <li>■ Fails on the <i>old</i> VSX Cluster Member <b>M1</b> with a warning. <b>Ignore this warning</b>.</li> </ul>

#### 6. On each VSX Cluster Member, examine the VSX configuration and cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	Examine the VSX configuration: <pre>vsx stat -v</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>

Step	Instructions
4	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish (R80.20 and higher), run:</li> </ul> <pre>set virtual-system 0 show cluster state</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode, run:</li> </ul> <pre>vsenv 0 cphaprof state</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ The cluster states of the upgraded VSX Cluster Members <b>M2</b> and <b>M3</b> are <b>Ready</b>.</li> <li>■ The cluster state of the old VSX Cluster Member <b>M1</b> is: <ul style="list-style-type: none"> <li>• In R80.20 and higher - <b>Active(!)</b>.</li> <li>• In R80.10 and lower - <b>Active Attention.</b></li> </ul> </li> </ul>

## 7. On the old VSX Cluster Member M1, stop all Check Point services

Step	Instructions
1	Connect to the command line on the VSX Cluster Member <b>M1</b> .
2	<p>Stop all Check Point services:</p> <pre>cpstop</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ This forces a controlled cluster failover from the old VSX Cluster Member <b>M1</b> to one of the upgraded VSX Cluster Members.</li> <li>■ At this moment, all connections that were initiated through the old VSX Cluster Member <b>M1</b> are dropped (because VSX Cluster Members with different software versions cannot synchronize).</li> </ul>

## 8. On the upgraded VSX Cluster Members M2 and M3, examine the cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member <b>M2</b> and <b>M3</b> .

Step	Instructions
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: <code>show cluster state</code></li> <li>■ In the Expert mode, run: <code>cphaprof state</code></li> </ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ One of the VSX Cluster Members (<b>M2 or M3</b>) changes its cluster state to <b>Active</b>.</li> <li>■ The other VSX Cluster Member (<b>M2 or M3</b>) changes its cluster state to <b>Standby</b>.</li> </ul>

9. **On the old VSX Cluster Member M1, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40**



**Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>.</p> <p>See <a href="#">sk92449</a> for detailed steps.</p>

Installation Method	Instructions
Clean Install of R80.40 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160. Follow the applicable action plan for the local or central installation. In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</li> </ol> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>
Clean Install of R80.40 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Follow "<a href="#">Installing a VSX Cluster</a>" on page 123 - only the step "Install the VSX Cluster Members".</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</li> </ol> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

## 10. In SmartConsole, install the policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Install the default policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the default policy for this VSX Cluster object. This policy is called:  <div style="border: 1px solid black; padding: 2px; display: inline-block;">&lt;Name of VSX Cluster object&gt;_VSX</div> </li> <li>In the <b>Install Mode</b> section, select these two options: <ul style="list-style-type: none"> <li>■ <b>Install on each selected gateway independently</b></li> <li>■ <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b></li> </ul> </li> <li>Click <b>Install</b>.</li> <li>The default policy install successfully on all the VSX Cluster Members.</li> </ol>
4	<p>Install the Threat Prevention Policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable Threat Prevention Policy for this VSX Cluster object.</li> <li>Click <b>Install</b>.</li> <li>The Threat Prevention Policy must install successfully on all the VSX Cluster Members.</li> </ol>

#### 11. On each VSX Cluster Member, examine the VSX configuration and cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	<p>Examine the VSX configuration:</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">vsx stat -v</div> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>

Step	Instructions
4	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> </ul> <pre data-bbox="520 316 859 384">set virtual-system 0 show cluster state</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode, run:</li> </ul> <pre data-bbox="520 451 759 518">vsenv 0 cphaprof state</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members.</li> <li>■ In the High Availability mode, one VSX Cluster Member must be in the <b>Active</b> state, and all other VSX Cluster Members must be in <b>Standby</b> state.</li> <li>■ In the Virtual System Load Sharing mode, all VSX Cluster Members must be in the <b>Active</b> state.</li> <li>■ All Virtual Systems must show the same information about the states of all Virtual Systems.</li> </ul>
5	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> </ul> <pre data-bbox="520 1136 1113 1203">set virtual-system 0 show cluster members interfaces all</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode, run:</li> </ul> <pre data-bbox="520 1271 759 1338">vsenv 0 cphaprof -a if</pre>

## 12. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or each <i>Target</i> Domain Management Server that manages the Virtual Systems on this VSX Cluster.
2	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .
3	Examine the logs from the Virtual Systems on this VSX Cluster to make sure they inspect the traffic as expected.

For more information, see the:

- [R80.40 VSX Administration Guide](#).
- [R80.40 CLI Reference Guide](#).

# Multi-Version Cluster (MVC) Upgrade

The Multi-Version Cluster (MVC) mechanism synchronizes connections between Cluster Members that run different versions.

You can upgrade to a newer version without a loss in connectivity and test the new version on some of the Cluster Members before you decide to upgrade the rest of the Cluster Members.



**Important** - The Multi-Version Cluster Upgrade replaced the Connectivity Upgrade.

## Multi-Version Cluster Upgrade Prerequisites



**Important** - Before you upgrade a cluster, follow the steps below.

Step	Instructions
1	<p>On each Cluster Member, run:</p> <pre>cphaprof state</pre> <p>a. All Cluster Members must be operational:</p> <ul style="list-style-type: none"> <li>■ In the High Availability mode:           <ul style="list-style-type: none"> <li>One Cluster Member must be in the <b>Active</b> state</li> <li>All other Cluster Members must be in the <b>Standby</b> state</li> </ul> </li> <li>■ In the Load Sharing mode:           <ul style="list-style-type: none"> <li>All Cluster Members must be in the <b>Active</b> state</li> </ul> </li> </ul> <p>b. All Cluster Members must agree upon the states of all Cluster Members.</p>
2	<p>Back up your current configuration (see "<a href="#">Backing Up and Restoring</a>" on page 27).</p> <p> <b>Important</b> - If you upgrade a VSX Cluster, then back up both the Management Server and the VSX Cluster Members. Follow <a href="#">sk100395: How to backup and restore VSX Gateway</a>.</p>
3	<p>See "<a href="#">Upgrade Options and Prerequisites</a>" on page 163.</p>
4	<p>See "<a href="#">Supported Versions in Multi-Version Cluster</a>" on the next page to know if you must install a Jumbo Hotfix Accumulator.</p>
5	<p>See "<a href="#">Planning a Cluster Upgrade</a>" on page 539.</p>
6	<p>You must upgrade the Management Server and Log Servers.</p> <ul style="list-style-type: none"> <li>■ See "<a href="#">Upgrade of Security Management Servers and Log Servers</a>" on page 185.</li> <li>■ See "<a href="#">Upgrade of Multi-Domain Servers and Multi-Domain Log Servers</a>" on page 271.</li> </ul>
7	<p><b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b></p>

## Supported Versions in Multi-Version Cluster

The Multi-Version Cluster (MVC) in an R80.40 Cluster Member supports synchronization with peer Cluster Members that run one of these versions:

- R80.10 (or higher)\*
- R77.30

In a Multi-Version Cluster, the Cluster Members can run only these versions:

- R80.40 and R80.10 (or higher)\*
- R80.40 and R77.30

\*For supported upgrade paths, see the [R80.40 Release Notes](#).

These scenarios are supported in Multi-Version Cluster:

- **There are only two Cluster Members in the Multi-Version Cluster**

The supported combination is:

Member 1	Member 2
R80.40	<i>Version X</i>

"*Version X*" is allowed to be only **one of these**: R77.30, R80.10, R80.20, and so on.

For supported upgrade paths, see the [R80.40 Release Notes](#).

- **There are three, four, or five Cluster Members in the Multi-Version Cluster**



**Important** - In this scenario, Jumbo Hotfix Accumulator is required:

- On Cluster Members R80.20, you must install R80.20 Jumbo Hotfix Accumulator Take 75 or higher (see [sk137592](#)).
- On Cluster Members R80.10, you must install R80.10 Jumbo Hotfix Accumulator Take 215 or higher (see [sk116380](#)).

The table shows the allowed combinations of Cluster Member versions:

Member 1	Member 2	Member 3	Member 4	Member 5
R80.40	<i>Version X</i>	<i>Version X</i>	<i>Version X</i>	<i>Version X</i>
R80.40	R80.40	<i>Version X</i>	<i>Version X</i>	<i>Version X</i>
R80.40	R80.40	R80.40	<i>Version X</i>	<i>Version X</i>
R80.40	R80.40	R80.40	R80.40	<i>Version X</i>

"*Version X*" is allowed to be only **one of these**: R77.30, R80.10, R80.20, and so on.

For supported upgrade paths, see the [R80.40 Release Notes](#).

## Multi-Version Cluster Limitations

Specific limitations apply to Multi-Version Cluster.

### General limitations in Multi-Version Cluster configuration

- While the cluster contains Cluster Members that run different software versions (Multi-Version Cluster), it is **not** supported to change specific settings of the cluster object in SmartConsole.

- You cannot change the cluster mode.

For example, from High Availability to Load Sharing.

- In the High Availability mode, you cannot change the recovery mode.

For example, from **Maintain current active Cluster Member** to **Switch to higher priority Cluster Member**.

- You cannot change the cluster topology.

Do **not** add, remove, or edit settings of cluster interfaces (IP addresses, Network Objectives, and so on).

In a VSX Cluster object, do **not** add, remove, or edit static routes.



**Note** - You can change these settings either before or after you upgrade all the Cluster Members.

- While the cluster contains Cluster Members that run different software versions (Multi-Version Cluster), you must install the policy two times.

## Procedure



**Important** - In a VSX Cluster, it is possible to install policy **only** on the *upgraded* VSX Cluster Members that run R80.40. After you change the version of the VSX Cluster object to R80.40, the Management Server does not let you change it to the previous version.

1. Make the required changes in the Access Control or Threat Prevention policy.
2. In SmartConsole, change the version of the cluster object to R80.40:

On the **General Properties** page > in the **Platform** section > in the **Version** field, select **R80.40** > click **OK**.

3. Install policy on the *upgraded* Cluster Members that run R80.40:
  - a. In the **Policy** field, select the applicable policy.
  - b. In the **Install Mode** section, select these two options:
    - Select **Install on each selected gateway independently**.
    - Clear **For gateway clusters, if installation on a cluster member fails, do not install on that cluster**.
  - c. Click **Install**.

The Policy installation:

- Succeeds on the *upgraded* R80.40 Cluster Members.
- Fails on the *old* Cluster Members with a warning. **Ignore this warning**.

4. In SmartConsole, change the version of the cluster object to the previous version:

On the **General Properties** page > in the **Platform** section > in the **Version** field, select the previous version > click **OK**.

5. Install policy on the *old* Cluster Members that run the previous version:
  - a. In the **Policy** field, select the applicable policy.
  - b. In the **Install Mode** section, select these two options:
    - Select **Install on each selected gateway independently**.
    - Clear **For gateway clusters, if installation on a cluster member fails, do not install on that cluster**.
  - c. Click **Install**.

The Policy installation:

- Succeeds on the *old* Cluster Members.
- Fails on the *upgraded* R80.40 Cluster Members with a warning. **Ignore this warning**.

## Limitations during failover in Multi-Version Cluster

These connections do **not** survive failover between Cluster Members with different versions:

- VPN:
  - During a cluster failover from an R80.40 Cluster Member to an R77.30 Cluster Member, all VPN connections on an R80.40 Cluster Member that are inspected on CoreXL Firewall instances #1 and higher, are lost.
  - Mobile Access VPN connections.
  - Remote Access VPN connections.
  - VPN Traditional Mode connections.
- Static NAT connections are cut off during a cluster failover from an R80.40 Cluster Member to an R80.10 or R77.30 Cluster Member, if VMAC mode is enabled in this cluster.
- Identity Awareness connections.
- Data Loss Prevention (DLP) connections.
- IPv6 connections.
- Threat Emulation connections.
- PSL connections that are open during fail-over and then fail-back.

In addition, see the [\*R80.40 ClusterXL Administration Guide\*](#) > Chapter *High Availability and Load Sharing Modes in ClusterXL* > Section *Cluster Failover*.

## Multi-Version Cluster Upgrade Procedure - Gateway Mode



**Note** - The procedure below is for ClusterXL and VRRP Cluster. For VSX Cluster, see "["Multi-Version Cluster Upgrade Procedure - VSX Mode" on page 596.](#)

**Important** - Before you upgrade a Cluster:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See " <a href="#">Upgrade Options and Prerequisites" on page 163</a> .
3	Upgrade the Management Server and Log Servers.
4	See " <a href="#">Planning a Cluster Upgrade" on page 539</a> .
5	<b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b>



**Note** - MVC supports Cluster Members with different Gaia kernel editions (R80.40 64-bit and R77.30 / R80.10 32-bit).

The procedure described below is based on an example cluster with three Cluster Members M1, M2 and M3.

However, you can use it for clusters that consist of two or more.

#### Action plan:

1. In SmartConsole, change the cluster object version to R80.40.
2. On the Cluster Member **M3**:
  - a. Upgrade to R80.40

**Note** - If you perform a Clean Install of R80.40, then you must establish SIC in SmartConsole with this Cluster Member
  - b. Enable the MVC
3. In SmartConsole, install the Access Control Policy on the Cluster Member **M3**.
4. On the next Cluster Member **M2**:
  - a. Upgrade to R80.40

**Note** - If you perform a Clean Install of R80.40, then you must establish SIC in SmartConsole with this Cluster Member
  - b. Enable the MVC
5. In SmartConsole, install the Access Control Policy on the Cluster Member **M3** and **M2**.
6. On the remaining Cluster Member **M1**:
  - Upgrade to R80.40

**Note** - If you perform a Clean Install of R80.40, then you must establish SIC in SmartConsole with this Cluster Member
7. In SmartConsole, install the Access Control Policy and the Threat Prevention Policy on the Cluster object.

**Procedure:**

- In SmartConsole, change the version of the cluster object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Cluster object.
4	From the left tree, click the <b>General Properties</b> page.
5	In the <b>Platform</b> section > <b>Version</b> field, select <b>R80.40</b> .
6	Click <b>OK</b> to close the <b>Gateway Cluster Properties</b> window.

- On the Cluster Member M3, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40**



**Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p>

Installation Method	Instructions
Clean Install of R80.40 from scratch	<p><b>Installing a Cluster Member</b>  Follow "<a href="#">Installing a ClusterXL Cluster</a>" on page 105 - only the step "<i>Install the Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p><b>Installing a VRRP Cluster Member</b>  Follow "<a href="#">Installing a VRRP Cluster</a>" on page 129 - only the step "<i>Install the VRRP Cluster Members</i>".</p> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p>

### 3. In SmartConsole, establish SIC with the Cluster Member M3



**Important** - This step is required only if you performed a Clean Install of R80.40 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main Domain Management Server</i> that manages this Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the cluster object.
4	From the left tree, click <b>Cluster Members</b> .
5	Select the object of this Cluster Member.
6	Click <b>Edit</b> .
7	On the <b>General</b> tab, click the <b>Communication</b> button.
8	Click <b>Reset</b> .
9	In the <b>One-time password</b> field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the <b>Confirm one-time password</b> field, enter the same Activation Key again.
11	Click <b>Initialize</b> .
12	The <b>Trust state</b> field must show <b>Trust established</b> .
13	Click <b>Close</b> to close the <b>Communication</b> window.
14	Click <b>OK</b> to close the <b>Cluster Member Properties</b> window.
15	Publish the SmartConsole session.

#### 4. On the R80.40 Cluster Member M3, enable the MVC mechanism

Step	Instructions
1	Connect to the command line on the Cluster Member.
2	Enable the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish: set cluster member mvc on</li> <li>■ In the Expert mode: cphaconf mvc on</li> </ul>
3	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish: show cluster members mvc</li> <li>■ In the Expert mode: cphaprobc mvc</li> </ul>

#### 5. In SmartConsole, install the Access Control Policy on the R80.40 Cluster Member M3

Step	Instructions
1	Click <b>Install Policy</b> .
2	In the <b>Install Policy</b> window: <ol style="list-style-type: none"> <li>a. In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>b. In the <b>Install Mode</b> section, select these two options: <ul style="list-style-type: none"> <li>■ Select <b>Install on each selected gateway independently</b>.</li> <li>■ Clear <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b>.</li> </ul> </li> <li>c. Click <b>Install</b>.</li> </ol>
3	The Access Control Policy installation: <ul style="list-style-type: none"> <li>■ Succeeds on the <i>upgraded</i> Cluster Member M3.</li> <li>■ Fails on the <i>old</i> Cluster Members M1 and M2 with a warning. Ignore this warning.</li> </ul>

## 6. On each Cluster Member, examine the cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Examine the cluster state in one of these ways: <ul style="list-style-type: none"><li>■ In Gaia Clish, run:<pre>show cluster state</pre></li><li>■ In the Expert mode, run:<pre>cphaprof state</pre></li></ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"><li>■ In the High Availability mode, one of the upgraded Cluster Members (<b>M2</b> or <b>M3</b>) changes its cluster state to <b>Active</b>. The other upgraded Cluster Member (<b>M2</b> or <b>M3</b>) changes its cluster state to <b>Standby</b>.</li><li>■ In the Load Sharing modes, all Cluster Members must be in the <b>Active</b> state.</li></ul>

7. On the Cluster Member M2, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p>
Clean Install of R80.40 from scratch	<p><b>Installing a Cluster Member</b></p> <p>Follow "<a href="#">Installing a ClusterXL Cluster</a>" on page 105 - only the step "<i>Install the Cluster Members</i>".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p><b>Installing a VRRP Cluster Member</b></p> <p>Follow "<a href="#">Installing a VRRP Cluster</a>" on page 129 - only the step "<i>Install the VRRP Cluster Members</i>".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p>

## 8. In SmartConsole, establish SIC with the Cluster Member M2



**Important** - This step is required only if you performed a Clean Install of R80.40 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main Domain Management Server</i> that manages this Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the cluster object.
4	From the left tree, click <b>Cluster Members</b> .
5	Select the object of this Cluster Member.
6	Click <b>Edit</b> .
7	On the <b>General</b> tab, click the <b>Communication</b> button.
8	Click <b>Reset</b> .
9	In the <b>One-time password</b> field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the <b>Confirm one-time password</b> field, enter the same Activation Key again.
11	Click <b>Initialize</b> .
12	The <b>Trust state</b> field must show <b>Trust established</b> .
13	Click <b>Close</b> to close the <b>Communication</b> window.
14	Click <b>OK</b> to close the <b>Cluster Member Properties</b> window.
15	Publish the SmartConsole session.

**9. On the R80.40 Cluster Member M2, enable the MVC mechanism**

Step	Instructions
1	Connect to the command line on the Cluster Member.
2	Enable the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:               <pre>set cluster member mvc on</pre> </li> <li>■ In the Expert mode:               <pre>cphaconf mvc on</pre> </li> </ul>
3	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:               <pre>show cluster members mvc</pre> </li> <li>■ In the Expert mode:               <pre>cphaprof mvc</pre> </li> </ul>

**10. In SmartConsole, install the Access Control Policy on the R80.40 Cluster Members M3 and M2**

Step	Instructions
1	Click <b>Install Policy</b> .
2	In the <b>Install Policy</b> window: <ol style="list-style-type: none"> <li>In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>In the <b>Install Mode</b> section, select these two options:               <ul style="list-style-type: none"> <li>■ Select <b>Install on each selected gateway independently</b>.</li> <li>■ Clear <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b>.</li> </ul> </li> <li>Click <b>Install</b>.</li> </ol>
3	The Access Control Policy installation: <ul style="list-style-type: none"> <li>■ Succeeds on the <i>upgraded</i> Cluster Members M3 and M2.</li> <li>■ Fails on the <i>old</i> Cluster Member M1 with a warning. <b>Ignore this warning</b>.</li> </ul>

**11. On each Cluster Member, examine the cluster state**

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Examine the cluster state in one of these ways: <ul style="list-style-type: none"><li>■ In Gaia Clish, run:<pre>show cluster state</pre></li><li>■ In the Expert mode, run:<pre>cphaprof state</pre></li></ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"><li>■ In the High Availability mode, one of the upgraded Cluster Members (<b>M2</b> or <b>M3</b>) changes its cluster state to <b>Active</b>. The other upgraded Cluster Member (<b>M2</b> or <b>M3</b>) changes its cluster state to <b>Standby</b>.</li><li>■ In the Load Sharing modes, all Cluster Members must be in the <b>Active</b> state.</li></ul>

12. On the old Cluster Member M1, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p>
Clean Install of R80.40 from scratch	<p><b>Installing a Cluster Member</b></p> <p>Follow "<a href="#">Installing a ClusterXL Cluster</a>" on page 105 - only the step "<i>Install the Cluster Members</i>".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p><b>Installing a VRRP Cluster Member</b></p> <p>Follow "<a href="#">Installing a VRRP Cluster</a>" on page 129 - only the step "<i>Install the VRRP Cluster Members</i>".</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p>

### 13. In SmartConsole, establish SIC with the Cluster Member M1



**Important** - This step is required only if you performed a Clean Install of R80.40 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or <i>Main Domain Management Server</i> that manages this Cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the cluster object.
4	From the left tree, click <b>Cluster Members</b> .
5	Select the object of this Cluster Member.
6	Click <b>Edit</b> .
7	On the <b>General</b> tab, click the <b>Communication</b> button.
8	Click <b>Reset</b> .
9	In the <b>One-time password</b> field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the <b>Confirm one-time password</b> field, enter the same Activation Key again.
11	Click <b>Initialize</b> .
12	The <b>Trust state</b> field must show <b>Trust established</b> .
13	Click <b>Close</b> to close the <b>Communication</b> window.
14	Click <b>OK</b> to close the <b>Cluster Member Properties</b> window.
15	Publish the SmartConsole session.

**14. In SmartConsole, install the Access Control Policy and Threat Prevention Policy on the Cluster object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Install the Access Control Policy: a. Click <b>Install Policy</b> . b. In the <b>Policy</b> field, select the applicable Access Control Policy. c. In the <b>Install Mode</b> section, select these two options: ■ <b>Install on each selected gateway independently</b> ■ <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b> d. Click <b>Install</b> . e. The Access Control Policy must install successfully on all the Cluster Members.
4	Install the Threat Prevention Policy: a. Click <b>Install Policy</b> . b. In the <b>Policy</b> field, select the applicable Threat Prevention Policy. c. Click <b>Install</b> . d. The Threat Prevention Policy must install successfully on all the Cluster Members.

**15. On each Cluster Member, examine the cluster state**

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Examine the cluster state in one of these ways: ■ In Gaia Clish, run: <pre>show cluster state</pre> ■ In the Expert mode, run: <pre>cphaprof state</pre>  <b>Important:</b> <ul style="list-style-type: none"> <li>■ All Cluster Members must show the same information about the states of all Cluster Members.</li> <li>■ In the High Availability mode, one Cluster Member must be in the <b>Active</b> state, and all other Cluster Members must be in <b>Standby</b> state.</li> <li>■ In the Load Sharing modes, all Cluster Members must be in the <b>Active</b> state.</li> </ul>

## 16. On each Cluster Member, disable the MVC mechanism

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	Disable the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">set cluster member mvc off</div> <li>■ In the Expert mode:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">cphaconf mvc off</div> </ul>
3	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">show cluster members mvc</div> <li>■ In the Expert mode:</li> <div style="border: 1px solid black; padding: 5px; margin-left: 20px;">cphaprof mvc</div> </ul>

## 17. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .
3	Examine the logs from this Cluster to make sure it inspects the traffic as expected.

For more information, see the:

- [R80.40 ClusterXL Administration Guide](#).
- [R80.40 VSX Administration Guide](#).

## Multi-Version Cluster Upgrade Procedure - VSX Mode



**Note** - The procedure below is for VSX Cluster. For ClusterXL and VRRP Cluster, see ["Multi-Version Cluster Upgrade Procedure - Gateway Mode" on page 581](#).

**Important** - Before you upgrade a VSX Cluster:

Step	Instructions
1	Back up your current configuration (see <a href="#">"Backing Up and Restoring" on page 27</a> ).
2	See <a href="#">"Upgrade Options and Prerequisites" on page 163</a> .
3	Upgrade the Management Server and Log Servers.
4	See <a href="#">"Planning a Cluster Upgrade" on page 539</a> .
5	<b>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</b>



**Note** - MVC supports VSX Cluster Members with different Gaia kernel editions (R80.40 64-bit and R77.30 / R80.10 32-bit).

The procedure described below is based on an example cluster with three VSX Cluster Members M1, M2 and M3.

However, you can use it for clusters that consist of two or more.

#### Action plan:

1. On the Management Server, upgrade the VSX Cluster object to R80.40.
2. On the VSX Cluster Member **M3**:
  - a. Upgrade to R80.40

**Note** - If you perform a Clean Install of R80.40, then push the VSX configuration from the Management Server to this VSX Cluster Member
  - b. Enable the MVC
3. In SmartConsole, install the Access Control Policy on the R80.40 VSX Cluster Member **M3**
4. On the next VSX Cluster Member **M2**:
  - a. Upgrade to R80.40

**Note** - If you perform a Clean Install of R80.40, then push the VSX configuration from the Management Server to this VSX Cluster Member
  - b. Enable the MVC
5. In SmartConsole, install the Access Control Policy on the R80.40 VSX Cluster Members **M3** and **M2**.
6. On the remaining VSX Cluster Member **M1**:
  - Upgrade to R80.40

**Note** - If you perform a Clean Install of R80.40, then push the VSX configuration from the Management Server to this VSX Cluster Member
7. In SmartConsole, install the Access Control Policy and the Threat Prevention Policy on the VSX Cluster object.
8. In SmartConsole, install the Access Control Policy and the Threat Prevention Policy on each Virtual System object.

**Procedure:****1. On the Management Server, upgrade the VSX Cluster object to R80.40**

Follow the [R80.40 VSX Administration Guide](#) > Chapter *Command Line Reference* > Section *vsx\_util* > Section *vsx\_util upgrade*.

**2. On the VSX Cluster Member M3, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40**

**Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li data-bbox="584 952 1451 1096">a. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</li> </ol> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li data-bbox="584 1244 1419 1423">b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p><b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li data-bbox="584 1558 1451 1731">c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li data-bbox="673 1590 1133 1648">■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li data-bbox="673 1653 1387 1688">■ Settings manually defined in various configuration files.</li> <li data-bbox="673 1693 1229 1729">■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

Installation Method	Instructions
Clean Install of R80.40 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Follow "<a href="#">Installing a VSX Cluster</a> on page 123 - only the step "Install the VSX Cluster Members".</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

3. On each VSX Cluster Member, examine the VSX configuration and cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	Examine the VSX configuration: <pre>vsx stat -v</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre>set virtual-system 0 show cluster state</pre> </li> <li>■ In the Expert mode, run:           <pre>vsenv 0 cphaprof state</pre> </li> </ul>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre>set virtual-system 0 show cluster members interfaces all</pre> </li> <li>■ In the Expert mode, run:           <pre>vsenv 0 cphaprof -a if</pre> </li> </ul>



**Important:**

- The upgraded VSX Cluster Member **M3** shows its cluster state as **Ready**.
- Other VSX Cluster Members **M2** and **M1** show the cluster state of the upgraded VSX Cluster Member **M3** as **Lost**, or do not detect it.
- All Virtual Systems must show the same information about the states of all Virtual Systems.

#### 4. On the R80.40 VSX Cluster Member M3, enable the MVC mechanism

Step	Instructions
1	Connect to the command line on the VSX Cluster Member.
2	Go to the context of Virtual System 0: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> </ul> <pre>set virtual-system 0</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode:</li> </ul> <pre>vsenv 0</pre>
3	Enable the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> </ul> <pre>set cluster member mvc on</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode:</li> </ul> <pre>cphaconf mvc on</pre>
4	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> </ul> <pre>show cluster members mvc</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode:</li> </ul> <pre>cphaprof mvc</pre>

#### 5. In SmartConsole, install the Access Control Policy on the R80.40 VSX Cluster Member M3

Step	Instructions
1	Click <b>Install Policy</b> .
2	In the <b>Install Policy</b> window: <ol style="list-style-type: none"> <li>In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>In the <b>Install Mode</b> section, select these two options: <ul style="list-style-type: none"> <li>■ Select <b>Install on each selected gateway independently</b>.</li> <li>■ Clear <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b>.</li> </ul> </li> <li>Click <b>Install</b>.</li> </ol>
3	The Access Control Policy installation: <ul style="list-style-type: none"> <li>■ Succeeds on the <i>upgraded</i> VSX Cluster Member M3.</li> <li>■ Fails on the <i>old</i> VSX Cluster Members M1 and M2 with a warning. <b>Ignore this warning</b>.</li> </ul>

## 6. On each VSX Cluster Member, examine the VSX configuration and cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	Examine the VSX configuration: <pre>vsx stat -v</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre>set virtual-system 0 show cluster state</pre> </li> <li>■ In the Expert mode, run:           <pre>vsenv 0 cphaprof state</pre> </li> </ul>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre>set virtual-system 0 show cluster members interfaces all</pre> </li> <li>■ In the Expert mode, run:           <pre>vsenv 0 cphaprof -a if</pre> </li> </ul>



**Important:**

- In High Availability mode:
  - The upgraded VSX Cluster Member **M3** changes its cluster state to **Active**.
  - Other VSX Cluster Members change their state to **Standby**.
- In the Virtual System Load Sharing mode:
  - The upgraded VSX Cluster Member **M3** changes its cluster state to **Active**.
  - Other VSX Cluster Members change their state to **Standby** and **Backup**.
- All Virtual Systems must show the same information about the states of all Virtual Systems.

7. On the VSX Cluster Member M2, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40



**Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li data-bbox="584 705 1451 848">a. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</li> </ol> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li data-bbox="584 990 1451 1163">b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p><b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li data-bbox="584 1304 1451 1477">c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li data-bbox="673 1343 1451 1401">■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li data-bbox="673 1401 1451 1432">■ Settings manually defined in various configuration files.</li> <li data-bbox="673 1432 1451 1464">■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

Installation Method	Instructions
Clean Install of R80.40 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Follow "<a href="#">Installing a VSX Cluster</a> on page 123 - only the step "Install the VSX Cluster Members".</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

## 8. On each VSX Cluster Member, examine the VSX configuration and cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	Examine the VSX configuration: <pre>vsx stat -v</pre> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre>set virtual-system 0 show cluster state</pre> </li> <li>■ In the Expert mode, run:           <pre>vsenv 0 cphaprof state</pre> </li> </ul>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:           <pre>set virtual-system 0 show cluster members interfaces all</pre> </li> <li>■ In the Expert mode, run:           <pre>vsenv 0 cphaprof -a if</pre> </li> </ul>



**Important:**

- In the High Availability mode:
  - One of the upgraded VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster state **Standby**.
- In the Virtual System Load Sharing mode:
  - One of the upgraded VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster states **Standby** and **Backup**.
- All Virtual Systems must show the same information about the states of all Virtual Systems.

**9. On the R80.40 VSX Cluster Member M2, enable the MVC mechanism**

Step	Instructions
1	Connect to the command line on the VSX Cluster Member.
2	Go to the context of Virtual System 0: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> </ul> <pre style="border: 1px solid black; padding: 5px;">set virtual-system 0</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode:</li> </ul> <pre style="border: 1px solid black; padding: 5px;">vsenv 0</pre>
3	Enable the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> </ul> <pre style="border: 1px solid black; padding: 5px;">set cluster member mvc on</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode:</li> </ul> <pre style="border: 1px solid black; padding: 5px;">cphaconf mvc on</pre>
4	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:</li> </ul> <pre style="border: 1px solid black; padding: 5px;">show cluster members mvc</pre> <ul style="list-style-type: none"> <li>■ In the Expert mode:</li> </ul> <pre style="border: 1px solid black; padding: 5px;">cphaprof mvc</pre>

**10. In SmartConsole, install the Access Control Policy on the R80.40 VSX Cluster Members M3 and M2**

Step	Instructions
1	Click <b>Install Policy</b> .
2	In the <b>Install Policy</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>b. In the <b>Install Mode</b> section, select these two options: <ul style="list-style-type: none"> <li>■ Select <b>Install on each selected gateway independently</b>.</li> <li>■ Clear <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b>.</li> </ul> </li> <li>c. Click <b>Install</b>.</li> </ul>
3	The Access Control Policy installation: <ul style="list-style-type: none"> <li>■ Succeeds on the <i>upgraded</i> VSX Cluster Members M3 and M2.</li> <li>■ Fails on the <i>old</i> VSX Cluster Member M1 with a warning. <b>Ignore this warning</b>.</li> </ul>

**11. On each VSX Cluster Member, examine the VSX configuration and cluster state**

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	Examine the VSX configuration: <pre>vsx stat -v</pre>  <b>Important:</b> <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:               <pre>set virtual-system 0 show cluster state</pre> </li> <li>■ In the Expert mode, run:               <pre>vsenv 0 cphaprof state</pre> </li> </ul>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:               <pre>set virtual-system 0 show cluster members interfaces all</pre> </li> <li>■ In the Expert mode, run:               <pre>vsenv 0 cphaprof -a if</pre> </li> </ul>



**Important:**

- In the High Availability mode:
  - One of the upgraded VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster state **Standby**.
- In the Virtual System Load Sharing mode:
  - One of the upgraded VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster states **Standby** and **Backup**.
- All Virtual Systems must show the same information about the states of all Virtual Systems.

**12. On the VSX Cluster Member M1, upgrade to R80.40 with CPUSE, or perform a Clean Install of R80.40**



**Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R80.40 with CPUSE	<p>See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</p> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Upgrade</b>. See <a href="#">sk92449</a> for detailed steps.</p>
Clean Install of R80.40 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li data-bbox="584 705 1451 848">a. See "<a href="#">Installing Software Packages on Gaia</a>" on page 160.</li> </ol> <p>Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</p> <p><b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li data-bbox="584 990 1451 1163">b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p><b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li data-bbox="584 1304 1451 1477">c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li data-bbox="673 1343 1133 1401">■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li data-bbox="673 1401 1387 1432">■ Settings manually defined in various configuration files.</li> <li data-bbox="673 1432 1229 1464">■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

Installation Method	Instructions
Clean Install of R80.40 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>a. Follow "<a href="#">Installing a VSX Cluster</a> on page 123 - only the step "Install the VSX Cluster Members".</li> </ol> <p> <b>Important</b> - In the Gaia First Time Configuration Wizard, for the <b>Management Connection</b> IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p> <ol style="list-style-type: none"> <li>b. Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member.</li> </ol> <p>See the <a href="#">R80.40 VSX Administration Guide</a> &gt; Chapter <i>Command Line Reference</i> &gt; Section <i>vsx_util</i> &gt; Section <i>vsx_util reconfigure</i>.</p> <p> <b>Important</b> - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member.</p> <ol style="list-style-type: none"> <li>c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> <li>■ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on).</li> <li>■ Settings manually defined in various configuration files.</li> <li>■ Applicable Check Point configuration files.</li> </ul> </li> </ol>

**13. On each VSX Cluster Member, examine the VSX configuration and cluster state**

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	Examine the VSX configuration: <pre>vsx stat -v</pre>  <b>Important:</b> <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:               <pre>set virtual-system 0 show cluster state</pre> </li> <li>■ In the Expert mode, run:               <pre>vsenv 0 cphaprof state</pre> </li> </ul>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:               <pre>set virtual-system 0 show cluster members interfaces all</pre> </li> <li>■ In the Expert mode, run:               <pre>vsenv 0 cphaprof -a if</pre> </li> </ul>



**Important:**

- In the High Availability mode:
  - One of the VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster state **Standby**.
- In the Virtual System Load Sharing mode:
  - One of the VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster states **Standby** and **Backup**.
- All Virtual Systems must show the same information about the states of all Virtual Systems.

**14. In SmartConsole, install the Access Control Policy and Threat Prevention Policy on the Cluster object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Install the Access Control Policy:</p> <ol style="list-style-type: none"> <li>a. Click <b>Install Policy</b>.</li> <li>b. In the <b>Policy</b> field, select the applicable Access Control Policy.</li> <li>c. In the <b>Install Mode</b> section, select these two options: <ul style="list-style-type: none"> <li>■ <b>Install on each selected gateway independently</b></li> <li>■ <b>For gateway clusters, if installation on a cluster member fails, do not install on that cluster</b></li> </ul> </li> <li>d. Click <b>Install</b>.</li> <li>e. The Access Control Policy must install successfully on all the Cluster Members.</li> </ol>
4	<p>Install the Threat Prevention Policy:</p> <ol style="list-style-type: none"> <li>a. Click <b>Install Policy</b>.</li> <li>b. In the <b>Policy</b> field, select the applicable Threat Prevention Policy.</li> <li>c. Click <b>Install</b>.</li> <li>d. The Threat Prevention Policy must install successfully on all the Cluster Members.</li> </ol>

**15. On each VSX Cluster Member, examine the VSX configuration and cluster state**

Step	Instructions
1	Connect to the command line on <i>each</i> VSX Cluster Member.
2	Log in to the Expert mode.
3	Examine the VSX configuration: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>vsx stat -v</pre> </div>
	<b>Important:</b>  <ul style="list-style-type: none"> <li>■ Make sure all the configured Virtual Devices are loaded.</li> <li>■ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.</li> </ul>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>set virtual-system 0 show cluster state</pre> </div> </li> <li>■ In the Expert mode, run:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>vsenv 0 cphaprof state</pre> </div> </li> </ul>
	<b>Important:</b>  <ul style="list-style-type: none"> <li>■ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members.</li> <li>■ In the High Availability mode, one VSX Cluster Member must be in the <b>Active</b> state, and all other VSX Cluster Members must be in <b>Standby</b> state.</li> <li>■ In the Virtual System Load Sharing mode, all VSX Cluster Members must be in the <b>Active</b> state.</li> <li>■ All Virtual Systems must show the same information about the states of all Virtual Systems.</li> </ul>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>set virtual-system 0 show cluster members interfaces all</pre> </div> </li> <li>■ In the Expert mode, run:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>vsenv 0 cphaprof -a if</pre> </div> </li> </ul>

**Important:**

- In the High Availability mode:
  - One of the VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster state **Standby**.
- In the Virtual System Load Sharing mode:
  - One of the VSX Cluster Members has the cluster state **Active**.
  - Other VSX Cluster Members have the cluster states **Standby** and **Backup**.
- All Virtual Systems must show the same information about the states of all Virtual Systems.

**16. On each VSX Cluster Member, disable the MVC mechanism**

Step	Instructions
1	Connect to the command line on each VSX Cluster Member.
2	Go to the context of Virtual System 0: <ul style="list-style-type: none"> <li>■ In Gaia Clish:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>set virtual-system 0</pre> </div> </li> <li>■ In the Expert mode:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>vsenv 0</pre> </div> </li> </ul>
3	Disable the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>set cluster member mvc off</pre> </div> </li> <li>■ In the Expert mode:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cphaconf mvc off</pre> </div> </li> </ul>
4	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> <li>■ In Gaia Clish:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>show cluster members mvc</pre> </div> </li> <li>■ In the Expert mode:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cphaprof mvc</pre> </div> </li> </ul>

**17. In SmartConsole, install the Access Control Policy and the Threat Prevention Policy on each Virtual System object**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or each <i>Target Domain</i> Management Server that manages the Virtual System on this VSX Cluster.
2	Install the Access Control Policy on the Virtual System object.
3	Install the Threat Prevention Policy on the Virtual System object.

## 18. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server or each <i>Target</i> Domain Management Server that manages the Virtual Systems on this VSX Cluster.
2	From the left navigation panel, click <b>Logs &amp; Monitor &gt; Logs</b> .
3	Examine the logs from the Virtual Systems on this VSX Cluster to make sure they inspect the traffic as expected.

For more information, see the:

- [R80.40 ClusterXL Administration Guide](#).
- [R80.40 VSX Administration Guide](#).

# Troubleshooting the Multi-Version Cluster

## Making sure the Cluster Members synchronize their connections

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	<p>Examine the Delta Synchronization statistics in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> <pre>show cluster statistics sync</pre> </ul> <ul style="list-style-type: none"> <li>■ In the Expert mode, run:</li> <pre>cphaprof syncstat</pre> </ul> <p>For more information, see the <a href="#">R80.40 ClusterXL Administration Guide</a> &gt; Chapter <i>Monitoring and Troubleshooting Clusters</i> - Section <i>ClusterXL Monitoring Commands</i> &gt; Section <i>Viewing Delta Synchronization</i>.</p>
3	<p>Examine the number of concurrent connections in the <b>Connections</b> kernel table (ID 8158). In the Expert mode, run:</p> <pre>fw tab -t connections -s</pre> <p> <b>Important</b> - These numbers must be as close as possible on all Cluster Members.</p> <p>For more information, see the <a href="#">R80.40 CLI Reference Guide</a>.</p>

## Collecting the cluster kernel debug

In case more detailed information is required, collect the kernel debug.

In the debug module "cluster", enable the debug flags "ccp" and "cu".

For complete debug procedure, see the [R80.40 Next Generation Security Gateway Guide](#) > Chapter *Kernel Debug on Security Gateway*.

# Upgrading a Full High Availability Cluster

For more information, see "[Full High Availability Cluster on Check Point Appliances](#)" on page 143.

To upgrade, follow the procedure "[Upgrading Security Management Servers in Management High Availability from R80.10 and lower](#)" on page 207.

**Important** - After you upgrade a Full High Availability Cluster to R80.40, you must establish the Secure Internal Communication (SIC) **again** between the Full High Availability Cluster Member that runs the Primary Security Management Server and the Full High Availability Cluster Member that runs the Secondary Security Management Server.



# Upgrading a Standalone from R80.10, R77.30 and lower

This section provides instructions to upgrade Standalone from R80.10 and lower:

- "[Upgrading a Standalone from R80.10 and lower with CPUSE](#)" on page 618
- "[Upgrading a Standalone from R80.10 and lower with Advanced Upgrade](#)" on page 621
- "[Upgrading a Standalone from R80.10 and lower with Migration](#)" on page 628

# Upgrading a Standalone from R80.10 and lower with CPUSE

In a CPUSE upgrade scenario, you perform the upgrade procedure on the same Standalone.

**Notes:**



- To upgrade from R80.20 or R80.30, see "[Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE](#)" on page 245.
- This upgrade method is supported only for servers that already run on Gaia Operating System.
- These instructions equally apply to:
  - Security Management Server
  - vSEC Controller R80.10 and lower

**Important - Before you upgrade a Standalone:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

**Procedure:****1. Upgrade the Standalone with CPUSE**

See "[Installing Software Packages on Gaia](#)" on page 160 and follow the applicable action plan.

**2. Install the R80.40 SmartConsole**

See "[Installing SmartConsole](#)" on page 89.

**3. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers**

If your Standalone manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Standalone:

- "[Upgrading a Dedicated Log Server from R80.10 and lower](#)" on page 212
- "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower](#)" on page 228

**4. Install the management database**

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

**5. Install the Event Policy**

**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Standalone.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Standalone.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .

Step	Instructions
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 6. Install the Security Policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	Click <b>Install Policy</b> .
3	Install the Access Control Policy on the Standalone object.
4	Install the Threat Prevention Policy on the Standalone object.

## 7. Test the functionality on the R80.40 Standalone

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Standalone from R80.10 and lower with Advanced Upgrade

In an advanced upgrade scenario, you perform the upgrade procedure on the same Standalone.

**Notes:**



- To upgrade from R80.20 or R80.30, see "[Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade](#)" on page 250.
- This upgrade method is supported only for servers that already run on Gaia Operating System.
- These instructions equally apply to:
  - Security Management Server
  - vSEC Controller R80.10 and lower

**Important - Before you upgrade a Standalone:**



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	See the " <a href="#">Upgrade Options and Prerequisites</a> " on page 163.
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current Standalone, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Standalone.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p> <b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Standalone, then export the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the current Standalone to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install the R80.40 Standalone

See the [R80.40 Release Notes](#) for requirements.

Do **not** perform initial configuration in SmartConsole.

Current OS	Available options
Gaia Operating System	<p>Follow one of these procedures:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Upgrading a Security Management Server or vSEC Controller from R80.10 and lower" on page 186</a></li> <li>■ <a href="#">"Installing a Standalone" on page 150</a></li> </ul>
Operating System other than Gaia	<p>Follow this procedure:</p> <ul style="list-style-type: none"> <li>■ <a href="#">"Installing a Security Management Server" on page 61</a></li> </ul>



**Important** - The IP address of the source and target Standalone servers **must be the same**. If it is necessary to have a different IP address on the R80.40 Standalone server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.

### 4. On the R80.40 Standalone, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Standalone.
2	Log in to the Expert mode.
3	Make sure a valid license is installed: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
4	Transfer the exported databases from an external storage to the R80.40 Standalone, to some directory.  <b>Note</b> - Make sure to transfer the files in the binary mode.
5	Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Standalone: <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	Go to the \$FWDIR/bin/upgrade_tools/ directory: <pre>cd \$FWDIR/bin/upgrade_tools/</pre>
7	Import the management database: <pre>yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre>  <b>Notes:</b> <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>

Step	Instructions
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ If you upgrade from R80 (or higher) version, and the IP addresses of the source and target Standalone <b>are different</b>:             <ol style="list-style-type: none"> <li>Issue licenses for the new IP address in your Check Point User Center account.</li> <li>Install the new licenses on the R80.40 Standalone.</li> </ol> </li> <li>■ If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Standalone <b>must be the same</b>.             <ul style="list-style-type: none"> <li>• If it is necessary to have a different IP address on the R80.40 Standalone, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.</li> </ul> </li> </ul>
8	 <p><b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Standalone, then import the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
9	Restart the Check Point services: <pre>cpstop cpstart</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

This step is part of the upgrade procedure of a Standalone server. If you upgrade a dedicated Log Server or SmartEvent Server, then skip this step.

If your Standalone manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Standalone:

- "[Upgrading a Dedicated Log Server from R80.10 and lower](#)" on page 212
- "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower](#)" on page 228

## 7. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.

Step	Instructions
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 8. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Standalone.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Standalone.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 9. Install the Security Policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	Click <b>Install Policy</b> .
3	Install the Access Control Policy on the Standalone object.
4	Install the Threat Prevention Policy on the Standalone object.

## 10. Test the functionality on the R80.40 Standalone

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	Make sure the management database and configuration were upgraded correctly.

# Upgrading a Standalone from R80.10 and lower with Migration

In a migration and upgrade scenario, you perform the procedure on the source Standalone and the different target Standalone.

**Notes:**



- To upgrade from R80.20 or R80.30, see "["Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 250.](#)
- This upgrade method is supported only for servers that already run on Gaia Operating System.
- These instructions equally apply to:
  - Security Management Server
  - vSEC Controller R80.10 and lower

**Important - Before you upgrade a Standalone:**

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring" on page 27</a> ).
2	See the " <a href="#">"Upgrade Options and Prerequisites" on page 163.</a>
3	In R80 and higher, examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>a. Connect with the SmartConsole to the Security Management Server.</li> <li>b. From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>c. You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
4	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the current Standalone, run the Pre-Upgrade Verifier and export the entire management database**

Step	Instructions
1	Connect to the command line on the current Standalone.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	 <b>Important</b> - This step applies only when you upgrade from R77.30 or lower.  Run the Pre-Upgrade Verifier (PUV). <ol style="list-style-type: none"> <li>Run this command and use the applicable syntax based on the instructions on the screen:   <pre>./pre_upgrade_verifier -h</pre></li> <li>Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> <li>Follow the instructions in the report.</li> <li>In a Management High Availability environment, if you made changes, synchronize the Management Servers immediately after these changes.</li> <li>Run the Pre-Upgrade Verifier again.</li> </ol> </li> </ol>

Step	Instructions
6	<p>Export the management database:</p> <pre>yes   nohup ./migrate export [-l   -x] [-n] &lt;Full Path&gt;/&lt;Name of Exported File&gt; &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
7	<p> <b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower.</p> <p>If <b>SmartEvent</b> Software Blade is enabled on this Standalone, then export the <b>Events</b> database. See <a href="#">sk110173</a>.</p>
8	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
9	<p>Transfer the exported databases from the current Standalone to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. Install a new R80.40 Standalone

Perform a clean install of the R80.40 Standalone on another computer.

Do **not** perform initial configuration in SmartConsole.

See "[Installing a Security Management Server](#)" on page 61.



**Important** - The IP address of the source and target Standalone **must be the same**. If it is necessary to have a different IP address on the R80.40 Standalone, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.

### 4. On the R80.40 Standalone, import the databases



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	Connect to the command line on the R80.40 Standalone.

Step	Instructions
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre data-bbox="414 339 1446 384">cplic print</pre>
	<p>If it is not already installed, then install a valid license now.</p>
4	<p>Transfer the exported databases from an external storage to the R80.40 Standalone, to some directory.</p>
	 <b>Note</b> - Make sure to transfer the files in the binary mode.
5	<p>Make sure the transferred files are not corrupted.</p>
	<p>Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the original Standalone:</p> <pre data-bbox="430 788 1224 833">md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Go to the \$FWDIR/bin/upgrade_tools/ directory:</p>
	<pre data-bbox="430 923 906 968">cd \$FWDIR/bin/upgrade_tools/</pre>
7	<p>Import the management database:</p>
	<pre data-bbox="430 1057 1271 1125">yes   nohup ./migrate import [-l   -x] [-n] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz &amp;</pre>
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Security Management Server Commands - Section <i>migrate</i>.</li> </ul>
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ If you upgrade from R80 (or higher) version, and the IP addresses of the source and target Standalone <b>are different</b>:       <ol style="list-style-type: none"> <li>a. Issue licenses for the new IP address in your Check Point User Center account.</li> <li>b. Install the new licenses on the R80.40 Standalone.</li> </ol> </li> <li>■ If you upgrade from R77.30 (or lower) version to R80.40, then the IP addresses of the source and target Standalone <b>must be the same</b>.       <ul style="list-style-type: none"> <li>• If it is necessary to have a different IP address on the R80.40 Standalone, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address.</li> </ul> </li> </ul>

Step	Instructions
8	 <b>Important</b> - This step applies only when you upgrade from R80, R77.30 or lower. If <b>SmartEvent</b> Software Blade is enabled on this Standalone, then import the <b>Events</b> database. See <a href="#">sk110173</a> .
9	Restart the Check Point services: <pre>cpstop cpstart</pre>

## 5. Install the R80.40 SmartConsole

See "[Installing SmartConsole](#)" on page 89.

## 6. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

This step is part of the upgrade procedure of a Standalone server. If you upgrade a dedicated Log Server or SmartEvent Server, then skip this step.

If your Standalone manages dedicated Log Servers or SmartEvent Servers, you must upgrade these dedicated servers to the same version as the Standalone:

- ["Upgrading a Dedicated Log Server from R80.10 and lower" on page 212](#)
- ["Upgrading a Dedicated SmartEvent Server from R80.10 and lower" on page 228](#)

## 7. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	In the top left corner, click <b>Menu &gt; Install database</b> .
3	Select all objects.
4	Click <b>Install</b> .
5	Click <b>OK</b> .

## 8. Install the Event Policy



**Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R80.40 Standalone.

Step	Instructions
1	Connect with the SmartConsole to the R80.40 Standalone.
2	In the SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
3	At the top, click <b>+</b> to open a new tab.
4	In the bottom left corner, in the <b>External Apps</b> section, click <b>SmartEvent Settings &amp; Policy</b> . The Legacy SmartEvent client opens.
5	In the top left corner, click <b>Menu &gt; Actions &gt; Install Event Policy</b> .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click <b>Close</b> .
9	Close the Legacy SmartEvent client.

## 9. Install the Security Policy

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	Click <b>Install Policy</b> .
3	Install the Access Control Policy on the Standalone object.
4	Install the Threat Prevention Policy on the Standalone object.

## 10. Test the functionality on the R80.40 Standalone

Step	Instructions
1	Connect with SmartConsole to the R80.40 Standalone.
2	Make sure the management database and configuration were upgraded correctly.

## 11. Disconnect the old Standalone from the network

Disconnect cables from the old Standalone.

## 12. Connect the new Standalone to the network

Connect cables to the new Standalone.

# Special Scenarios for Management Servers

This section describes various migration and configuration scenarios for Management Servers, such as migrating the database, backing up and restoring, and others.

# Backing Up and Restoring a Domain

You can back up a Domain and later restore it on the same Multi-Domain Server.

**Important:**



- You can restore a Domain *only* on the same Multi-Domain Server, on which you backed it up.
- You can restore a Domain, to which a Global Policy is assigned, *only* if during the Domain backup you did **not** purge the assigned Global Domain Revision.

## Backing Up a Domain

Run this API:

```
backup-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *backup-domain*.

## Restoring a Domain

### 1. Make sure it is possible to restore the Domain

Before you can restore a Domain, you must delete the current Domain.

Before you delete the current Domain, make sure it is possible to restore it.

Run this API with the "verify-only" flag:

```
restore-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *restore-domain*.

### 2. Delete the current Domain

Before you can restore a Domain, you must delete the current Domain.

You can perform this step in one of these ways:

- In SmartConsole connected to the **MDS** context
- With the API *delete domain* (see the [Check Point Management API Reference](#))

### 3. Restore the Active Domain Management Server

Run this API:

```
restore-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *restore-domain*.

### 4. Restore the Standby Domain Management Servers and Domain Log Servers

When you restore the Standby Domain Management Servers and Domain Log Servers, they must have the same IP addresses that were used when you collected the Domain backup.

For API documentation, see the [Check Point Management API Reference](#) - search for *set domain*

For each Standby Domain Management Server, run this API:

```
set-domain name <Name or UID of Domain> servers.add.ip-address <IP Address of Domain Management Server> servers.add.name <Name of Domain Management Server> servers.add.multi-domain-server <Name of Multi-Domain Server> servers.add.backup-file-path <Full Path to Domain Backup File>.tgz --format json
```

For each Domain Log Server, run this API:

```
set-domain name <Name or UID of Domain> servers.add.ip-address <IP Address of Domain Log Server> servers.add.name <Name of Domain Log Server> servers.add.multi-domain-server <Name of Multi-Domain Server> servers.add.backup-file-path <Full Path to Domain Backup File>.tgz --format json servers.add.type "log server"
```

## 5. Configure and assign the Administrators and GUI clients

You must again configure the Multi-Domain Server Administrators and GUI clients and assign them to the Domains.

a. Configure the Multi-Domain Server Administrators and GUI clients:

- i. Run the `mdsconfig` command
- ii. Configure the **Administrators**
- iii. Configure the **GUI clients**

b. Assign the Administrators and GUI clients to the Domains:

See the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter **Managing Domains** - Section **Creating a New Domain** and Section **Assigning Trusted Clients to Domains**.

## 6. Install policy on all managed Security Gateways and Clusters

- a. Connect with SmartConsole to the restored Active Domain.
- b. Install the applicable policies on all managed Security Gateways and Clusters.

# Migrating a Domain Management Server between R80.40 Multi-Domain Servers

This procedure lets you export the entire management database from a Domain Management Server on one R80.40 Multi-Domain Server and import it on another R80.40 Multi-Domain Server.

For the list of known limitations, see [sk156072](#).

## Procedure:

### 1. On the source Multi-Domain Server, export the Domain Management Server

- Run this API:

```
migrate-export-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *migrate-export-domain*.

- Calculate the MD5 of the export file:

```
md5sum <Full Path to Export File>
```

### 2. Transfer the export file to the target Multi-Domain Server

- Transfer the export file from the source Multi-Domain Server to the target Multi-Domain Server, to some directory.



**Note** - Make sure to transfer the file in the binary mode.

- Make sure the transferred file is not corrupted.

Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the source Multi-Domain Server:

```
md5sum <Full Path to Export File>
```

### 3. On the target Multi-Domain Server, import the Domain Management Server

- Run this API:

```
migrate-import-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *migrate-import-domain*.

- b. Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):

```
mdsstat
```

If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server and check again. Run these three commands:

```
mdsstopp_customer <IP Address or Name of Domain Management  
Server>  
mdsstart_customer <IP Address or Name of Domain Management  
Server>  
mdsstat
```

#### 4. Configure and assign the Administrators and GUI clients

You must again configure the Multi-Domain Server Administrators and GUI clients and assign them to the Domains.

- a. Configure the Multi-Domain Server Administrators and GUI clients:
  - i. Run the `mdsconfig` command
  - ii. Configure the **Administrators**
  - iii. Configure the **GUI clients**
  - iv. Exit the `mdsconfig` menu
- b. Assign the Administrators and GUI clients to the Domains:

See the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter **Managing Domains** - Section **Creating a New Domain** and Section **Assigning Trusted Clients to Domains**.

#### 5. Install policy on all managed Security Gateways and Clusters

- a. Connect with SmartConsole to the Active Domain (to which this Domain Management Server belongs).
- b. Install the applicable policies on all managed Security Gateways and Clusters.

# Migrating Database Between R80.40 Security Management Servers

This procedure lets you export the entire management database from one R80.40 Security Management Server and import it on another R80.40 Security Management Server.

**Important** - Before you migrate the database:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	Examine the SmartConsole sessions: <ol style="list-style-type: none"> <li>Connect with the SmartConsole to the Security Management Server.</li> <li>From the left navigation panel, click <b>Manage &amp; Settings &gt; Sessions &gt; View Sessions</b>.</li> <li>You must publish or discard all sessions, for which the <b>Changes</b> column shows a number greater than zero. Right-click on such session and select <b>Publish</b> or <b>Discard</b>.</li> </ol>
3	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

## Procedure:

- On the source R80.40 Security Management Server, export the entire management database

Step	Instructions
1	Connect to the command line on the current R80.40 Security Management Server.
2	Log in to the Expert mode.
3	Go to the \$FWDIR/scripts/ directory: <pre>cd \$FWDIR/scripts/</pre>

Step	Instructions
4	<p>Export the management database:</p> <p><b>If the "Endpoint Policy Management" blade is <i>disabled</i> on this Security Management Server</b></p> <ul style="list-style-type: none"> <li>And this Security Management Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] &lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>And this Security Management Server is <b>not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] &lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <p><b>If the "Endpoint Policy Management" blade is <i>enabled</i> on this Security Management Server</b></p> <ul style="list-style-type: none"> <li>This Security Management Server <i>is</i> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 [-l   -x] [--include-uepm-msi-files] &lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <ul style="list-style-type: none"> <li>This Security Management Server is <b>not</b> connected to the Internet, run:</li> </ul> <pre>./migrate_server export -v R80.40 -skip_upgrade_tools_check [-l   -x] [--include-uepm-msi-files] &lt;Full Path&gt;/&lt;Name of Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	<p>Transfer the exported databases from the source Security Management Server to an external storage:</p> <pre>&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 2. Install a new R80.40 Security Management Server

Step	Instructions
1	See the <a href="#">R80.40 Release Notes</a> for requirements.
2	Perform a clean install of the R80.40 Security Management Server on another computer. See " <a href="#">Installing a Security Management Server</a> " on page 61.



**Important** - The IP addresses of the source and target R80.40 servers **must be the same**. If it is necessary to have a different IP address on the R80.40 server, you can change it only after the upgrade procedure. Note that you have to issue licenses for the new IP address. For applicable procedures, see [sk40993](#) and [sk65451](#).

### 3. On the R80.40 Security Management Server, import the databases

Step	Instructions
1	Connect to the command line on the R80.40 Security Management Server.
2	Log in to the Expert mode.
3	Make sure a valid license is installed: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
4	Transfer the exported database from an external storage to the R80.40 Security Management Server, to some directory.  <b>Note</b> - Make sure to transfer the file in the binary mode.
5	Make sure the transferred files are not corrupted. Calculate the MD5 for the transferred files and compare them to the MD5 that you calculated on the source Security Management Server: <pre>md5sum /&lt;Full Path&gt;/&lt;Name of Database File&gt;.tgz</pre>
6	Go to the \$FWDIR/scripts/ directory: <pre>cd \$FWDIR/scripts/</pre>
7	Import the management database: <ul style="list-style-type: none"> <li>■ If this Security Management Server <i>is</i> connected to the Internet, run: <pre>./migrate_server import -v R80.40 [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> </li> <li>■ If this Security Management Server <b>is not</b> connected to the Internet, run: <pre>./migrate_server import -v R80.40 -skip_upgrade_tools_check [-l   -x] /&lt;Full Path&gt;/&lt;Name of Exported File&gt;.tgz</pre> </li> </ul>  <b>Important</b> - The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands). <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>

### 4. Test the functionality on the R80.40 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R80.40 Security Management Server.
2	Make sure the management database and configuration were upgraded correctly.

**5. Disconnect the old Security Management Server from the network**

Disconnect cables from the old Security Management Server.

**6. Connect the new Security Management Server to the network**

Connect cables to the new Security Management Server.

# Migrating Database from an R80.40 Security Management Server to an R80.40 Domain Management Server

This procedure lets you export the entire management database from an R80.40 Security Management Server and import it on an R80.40 Multi-Domain Server into a Domain Management Server.

For the list of known limitations, see [sk156072](#).

## Prerequisites on the source Security Management Server:

- Make sure to publish all changes you wish to migrate.
- Make sure all required processes are up and running:

```
cpwd_admin list
```

The "STAT" column must show "E" (executing) for all processes.

- Close the active Security log (`$_FWDIR/log/fw.log`) and Audit log (`$_FWDIR/log/fw.adtlog`) files:  

```
fw logswitch  
fw logswitch -audit
```
- If the target Domain Management Server must have a different IP address than the source Security Management Server, then you must prepare the source database before the export.

## Instructions in SmartConsole

1. Create a new **Host** object with the new IP address of the target Domain Management Server.

2. In each Security Policy, add a new Access Control rule to allow specific traffic from the **Host** object with new IP address to all managed Security Gateways and Clusters.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	Traffic from new Domain Management Server to managed Gateways	Host object with new IP address	Applicable objects of managed Security Gateways and Clusters	Any	FW1 FW1_CPRID CPD	Accept	None	Policy Targets

**Notes:**



- You must use the pre-defined Check Point services.
- If the source Security Management Server manages VSX Gateways or VSX Clusters, you must also add this Access Control rule to their default VSX policies.

These default policies are called:

*<Name of VSX Gateway or VSX Cluster Object>\_VSX*

3. Install all updated Access Control Policies.

#### Prerequisites on the target Multi-Domain Server:

- The free disk space must be at least 5 times the size of the database file you export from the source Security Management Server.
- Back up the current Multi-Domain Server. See "[Backing Up and Restoring](#)" on page 27.
- Do not create a new Domain Management Server on the target Multi-Domain Server. This procedure creates it automatically.
- Make sure you install the required license.

#### Procedure:

1. **On the source R80.40 Security Management Server, export the database**

- a. Run this API:

```
migrate-export-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *migrate-export-domain*.

Example:

```
mgmt_cli -d "System Data" migrate-export-domain file-path  
"/var/log/SecMgmtServer_Export.tgz" include-logs "false"
```

**Important** - The option *-d "System Data"* is mandatory.

- b. Calculate the MD5 of the export file:

```
md5sum <Full Path to Export File>.tgz
```

## 2. Transfer the export file to the target R80.40 Multi-Domain Server

- a. Transfer the export file from the source Security Management Server to the target Multi-Domain Server, to some directory.



**Note** - Make sure to transfer the file in the binary mode.

- b. Make sure the transferred file is not corrupted.

Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the source Security Management Server:

```
md5sum <Full Path to Export File>.tgz
```

## 3. On the target Multi-Domain Server, import the Security Management Server database into a Domain Management Server

- a. Make sure you have the sufficient license.
- b. Run this API:

```
migrate-import-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *migrate-import-domain*.

Make sure the name of the Domain you create does not conflict with the name of an existing Domain.

Example:

```
mgmt_cli -d "System Data" migrate-import-domain domain-name
"MyDomain3" domain-server-name "MyDomainServer3" domain-ip-
address "192.168.20.30" file-path "/var/log/SecMgmtServer_
Export.tgz" include-logs "false"
```

**Important** - The option *-d "System Data"* is mandatory.

- c. Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):

```
mdsstat
```

If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server and check again. Run these three commands:

```
mdsstop_customer <IP Address or Name of Domain Management
Server>
mdsstart_customer <IP Address or Name of Domain Management
Server>
mdsstat
```

#### 4. Configure and assign the Administrators and GUI clients

You must again configure the Multi-Domain Server Administrators and GUI clients and assign them to the new Domain.

- a. Configure the Multi-Domain Server Administrators and GUI clients:
  - i. Run the `mdsconfig` command.
  - ii. Configure the **Administrators**.
  - iii. Configure the **GUI clients**.
  - iv. Exit the `mdsconfig` menu.

- b. Assign the Administrators and GUI clients to the new Domain.

See the [R80.40 Multi-Domain Security Management Administration Guide](#) - Chapter **Managing Domains** - Section **Creating a New Domain** and Section **Assigning Trusted Clients to Domains**.

#### 5. Stop the source R80.40 Security Management Server

- a. Connect to the command line on the source Security Management Server.
- b. Stop the source Security Management Server you migrated:

```
cpstop
```

#### 6. Test the functionality on the R80.40 Domain Management Server

- a. Connect with SmartConsole to the Domain Management Server.
- b. Make sure the management database and configuration were imported correctly.

#### 7. Install policy on all managed Security Gateways and Clusters

In SmartConsole, install the applicable policies on all managed Security Gateways and Clusters.

#### 8. Disconnect the source R80.40 Security Management Server

Disconnect the source Security Management Server from the network.

#### 9. Delete the special Access Control rule you added before migration



**Important** - This step applies only if the target Domain Management Server has a different IP address than the source Security Management Server.

- a. Connect with SmartConsole to the target Domain Management Server.
- b. In each Security Policy, delete the Access Control rule with the new **Host** object you added on the source Security Management Server before migration.
- c. Delete the **Host** object you added on the source Security Management Server before migration.
- d. Install the applicable policies on all managed Security Gateways and Clusters.

# Migrating Database from an R80.40 Domain Management Server to an R80.40 Security Management Server

This procedure lets you export the entire management database from a Domain Management Server on an R80.40 Multi-Domain Server and import it on an R80.40 Security Management Server.

For the list of known limitations, see [sk156072](#).

### Prerequisites on the source Domain Management Server:

- Back up the current Multi-Domain Server. See "[Backing Up and Restoring" on page 27.](#)
- Make sure to publish all changes you wish to migrate.
- Close the active Security log (`$_FWDIR/log/fw.log`) and Audit log (`$_FWDIR/log/fw.adtlog`) files:

```
mdsenv <Name or IP Address of Domain Management Server>
fw logswitch
fw logswitch -audit
```

- If the target Security Management Server must have a different IP address than the source Domain Management Server, then you must prepare the source database before the export.

### Instructions in SmartConsole

1. Create a new **Host** object with the new IP address of the target Security Management Server.
2. In each Security Policy, add a new Access Control rule to allow specific traffic from the **Host** object with new IP address to all managed Security Gateways and Clusters.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	Traffic from new Security Management Server to managed Gateways	Host object with new IP address	Applicable objects of managed Security Gateways and Clusters	Any	FW1 FW1_CPRID CPD	Accept	None	Policy Targets

#### Notes:



- You must use the pre-defined Check Point services.
- If the source Domain Management Server manages VSX Gateways or VSX Clusters, you must also add this Access Control rule to their default VSX policies.  
These default policies are called:  
`<Name of VSX Gateway or VSX Cluster Object>_VSX`

3. Install all updated Access Control Policies.

### Prerequisites on the target Security Management Server:

- Perform a clean install of an R80.40 Security Management Server.

See "[Installing One Security Management Server only, or Primary Security Management Server in Management High Availability" on page 62.](#)

- Make sure you install the required license.

**Procedure:****1. On the source R80.40 Multi-Domain Server, export the Domain Management Server**

- Run this API:

```
migrate-export-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *migrate-export-domain*.

Example:

```
mgmt_cli -d "System Data" migrate-export-domain domain  
"MyDomain3" file-path "/var/log/MyDomain3_Export.tgz" include-  
logs "false"
```

**Important** - The option *-d "System Data"* is mandatory.

- Calculate the MD5 of the export file:

```
md5sum <Full Path to Export File>.tgz
```

**2. Transfer the export file to the target R80.40 Security Management Server**

- Transfer the export file from the source Multi-Domain Server to the target Security Management Server, to some directory.



**Note** - Make sure to transfer the file in the binary mode.

- Make sure the transferred file is not corrupted.

Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the source Multi-Domain Server:

```
md5sum <Full Path to Export File>.tgz
```

**3. On the target Security Management Server, import the Domain Management Server database**

Run the \$MDS\_FWDIR/scripts/migrate\_import\_domain.sh script.

In a plain-text editor, prepare the applicable syntax for your environment:

```
$MDS_FWDIR/scripts/migrate_import_domain.sh -sn <Name of New  
Security Management Server> -dsi <IP Address of New Security  
Management Server> -o <Full Path to Exported File>.tgz [-skip_logs]
```

## Parameters

Parameter	Description
<code>-sn &lt;Name of New Security Management Server&gt;</code>	Specifies a new name of the new Security Management Server object.
<code>-dsi &lt;IP Address of New Security Management Server&gt;</code>	Specifies a new IP Address of the new Security Management Server object.
<code>-o &lt;Full Path to Exported File&gt;.tgz</code>	Specifies the full path to the export file you transferred from the source R80.40 Multi-Domain Server.
<code>-skip_logs</code>	Optional. Specifies not to import log files \$FWDIR/log/fw.*log.

## 4. Configure and assign the Administrators and GUI clients

You must again configure the Security Management Server Administrators and GUI clients.

- Run the `cpconfig` command.
- Configure the **Administrators**.
- Configure the **GUI clients**.
- Exit the `cpconfig` menu.

## 5. Stop the source R80.40 Domain Management Server

- Connect to the command line on the source Multi-Domain Server.
- Stop the source Domain Management Server you migrated:

```
mdsstopp_customer <IP address or Name of Domain Management Server>
```

## 6. Test the functionality on the target R80.40 Security Management Server

- Connect with SmartConsole to the target Security Management Server.
- Make sure the management database and configuration were imported correctly.

## 7. Install policy on all managed Security Gateways and Clusters

In SmartConsole, install the applicable policies on all managed Security Gateways and Clusters.

## 8. Delete the source R80.40 Domain Management Server

Make sure you backed up the Multi-Domain Server. See ["Backing Up and Restoring" on page 27](#).

- Connect with SmartConsole to the source Multi-Domain Server to the **MDS** context.
- From the left navigation panel, click **Multi Domain > Domains**.
- Right-click the Domain Management Server object you migrated and select **Delete**.

## 9. Delete the special Access Control rule you added before migration



**Important** - This step applies only if the target Security Management Server has a different IP address than the source Domain Management Server.

- a. Connect with SmartConsole to the target Security Management Server.
- b. In each Security Policy, delete the Access Control rule with the new **Host** object you added on the source Domain Management Server before migration.
- c. Delete the **Host** object you added on the source Domain Management Server before migration.
- d. Install the applicable policies on all managed Security Gateways and Clusters.

# Migrating Global Policies from an R7x Multi-Domain Server

This procedure lets you export the Global Policies from an **R7x** Multi-Domain Server and import them to the **R80.40** Multi-Domain Server.

**Note** - This procedure is not supported for exporting the Global Policies from an **R8x** Multi-Domain Server.

**Important:**

- You must migrate the Global Policies before you migrate the databases from other Domains.
- You can migrate the Global Policies only one time from the R7x Multi-Domain Server.

**Procedure:**

1. **Install a new R80.40 Multi-Domain Server**

Step	Instructions
1      See the <a href="#">R80.40 Release Notes</a> for requirements.	
2      Perform the clean install in one of these ways: <b>Important</b> - Do not perform initial configuration in SmartConsole. <ul style="list-style-type: none"> <li>■ Follow "<a href="#">Installing Software Packages on Gaia</a>" on page 160 - select the R80.40 package and perform <b>Clean Install</b>. See <a href="#">sk92449</a> for detailed steps.</li> <li>■ Follow "<a href="#">Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability</a>" on page 71.</li> </ul>	



**Important** - Do not create Domains.

2. **Get the R80.40 Management Server Migration Tool**

Step	Instructions
1      Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <a href="#">Management Server Migration Tool and Upgrade Tools</a> " on page 182).	
2      Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, <code>/var/log/path_to_migration_tool/</code> ).  <b>Note</b> - Make sure to transfer the file in the binary mode.	

### 3. Export the global management database from the R7x Global Domain

Step	Instructions
1	Close all GUI clients (SmartConsole applications) connected to the R7x Multi-Domain Server.
2	Connect to the command line on the R7x Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.
5	Go to the directory, where you put the R80.40 Management Server Migration Tool package: <pre>cd /var/log/path_to_migration_tool/</pre>
6	Extract the R80.40 Management Server Migration Tool package: <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
7	Go to the main MDS context: <pre>mdsenv</pre>
8	Export the entire management database: <pre>yes   nohup ./migrate export [-f] [-n] /&lt;Full Path&gt;/R7x_global_policies &amp;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ <b>yes   nohup ... &amp;</b> are mandatory parts of the syntax.</li> <li>■ <b>R7x_global_policies</b> is the name of the export file.</li> <li>■ For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter Multi-Domain Security Management Commands - Section <i>migrate</i>.</li> </ul>
9	Calculate the MD5 for the exported database file: <pre>md5sum /&lt;Full Path&gt;/R7x_global_policies.tgz</pre>
10	Transfer the exported database from the R7x Multi-Domain Server to an external storage: <pre>/&lt;Full Path&gt;/R7x_global_policies.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 4. On the Primary R80.40 Multi-Domain Server, set the Global Domain to the Active state



**Note** - In Management High Availability environment, make sure the Global Domain is in the **Active** state on the **Primary** Multi-Domain Server.

Step	Instructions
1	Connect with SmartConsole to the IP address of the Primary R80.40 Multi-Domain Server. Select the <b>MDS</b> context.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	If the Global Domain on the Primary Multi-Domain Server is in the <b>Standby</b> state, then proceed to the next <b>Step 4</b> in this procedure. If the Global Domain on the Primary Multi-Domain Server is already in the <b>Active</b> state, then skip to the next <b>Step 5</b> in the main procedure.
4	Right-click the cell of the Global Domain, and select <b>Connect to Domain Server</b> .
5	In the Domain SmartConsole instance, in the top left corner, click <b>Menu &gt; Management High Availability</b> .
6	In the <b>High Availability Status</b> window, in the <b>Connected To</b> section, click <b>Actions &gt; Set Active</b> .
7	Close the Domain SmartConsole instance.

## 5. On the R80.40 Multi-Domain Server, remove all the global objects from the Global Domain



**Important** - This step applies *only* if you already configured global objects on the R80.40 Multi-Domain Server.

Step	Instructions
1	Connect with SmartConsole to the IP address of the Multi-Domain Server. Select the <b>MDS</b> context.
	 <b>Note</b> - In Multi-Domain Server High Availability environment, connect to the Primary Multi-Domain Server.
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	Right-click the cell of the Global Domain, and select <b>Connect to Domain Server</b> .
4	In the Domain SmartConsole instance, click <b>Objects</b> menu > <b>Object Explorer</b> .
5	Remove all the global objects.
6	Publish the SmartConsole session.
7	Close the Domain SmartConsole instance.

## 6. On the R80.40 Multi-Domain Server, import the R7x global management database to the Global Domain



**Important** - Before you import the management database, we strongly recommend to install the latest General Availability Take of the R80.40 Jumbo Hotfix Accumulator from [sk165456](#). This makes sure the R80.40 server has the latest improvements for reported import issues.

Step	Instructions
1	<p>Connect to the command line on the R80.40 Multi-Domain Server.</p> <p> <b>Note</b> - In Multi-Domain Server High Availability environment, connect to the Primary Multi-Domain Server.</p>
2	<p>Log in with the superuser credentials.</p>
3	<p>Log in to the Expert mode.</p>
4	<p>Make sure a valid license is installed:</p> <pre>mdsenv cplic print</pre> <p>If it is not already installed, then install a valid license now.</p>
5	<p>Transfer the exported database from an external storage to the R80.40 <b>Primary</b> Multi-Domain Server, to some directory.</p> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>
6	<p>Make sure the transferred file is not corrupted.</p> <p>Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the original R7x Multi-Domain Server:</p> <pre>md5sum &lt;Full Path&gt;/R7x_global_policies.tgz</pre>
7	<p>Go to the main MDS context:</p> <pre>mdsenv</pre>
8	<p>Import the global management database:</p> <pre>migrate_global_policies &lt;Full Path&gt;/R7x_global_policies.tgz</pre> <p> <b>Note</b> - This command stops the Multi-Domain Server.</p>
9	<p>Restart the Check Point services:</p> <pre>mdsstopp mdssstart</pre>

Step	Instructions
10	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server, and check again. Run these three commands:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 7. In R80.40 Multi-Domain Server High Availability, synchronize the global databases

Step	Instructions
1	<p>Connect with SmartConsole to the IP address of the Primary R80.40 Multi-Domain Server.</p> <p>Select the <b>MDS</b> context.</p>
2	From the left navigation panel, click <b>Multi-Domain &gt; Domains</b> .
3	Right-click the cell of the Global Domain Server in the <b>Active</b> state, and select <b>Connect to Domain Server</b> .
4	In the Domain SmartConsole instance, in the top left corner, click <b>Menu &gt; Management High Availability</b> .
5	<p>In the <b>High Availability Status</b> window, in the <b>Peers</b> section, click <b>Sync Peer</b>.</p>  <p><b>Note</b> - The synchronization operation can take many minutes to complete.</p>
6	Close the Domain SmartConsole instance.

# Migrating Database from an R7x Security Management Server to an R80.40 Domain Management Server

This procedure lets you export the entire management database from an **R7x** Security Management Server and import it to a new Domain Management Server on an R80.40 Multi-Domain Server.



**Note** - This procedure is **not** supported for exporting the management database from an R8x Security Management Server and importing it to an R80.40 Domain Management Server.

**Important** - Before you migrate the database:



Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).
2	Make sure that you are migrating the database only on one Domain Management Server. If you migrate a database to more than one Domain Management Server, the import fails and shows an error message.



**Important** - Before you import the database on the Secondary Multi-Domain Server in Management High Availability, you must change the state of its Global Domain to **Active**.

## Instructions

Step	Instructions
1	Connect with SmartConsole to the Secondary Multi-Domain Server.
2	From the left navigation panel, click <b>Multi Domain &gt; Domains</b> .
3	Right-click the Global Domain of the Secondary Multi-Domain Server and click <b>Connect to Domain</b> . A window shows for the Global Domain.
4	Click <b>Menu &gt; Management High Availability</b> . The <b>Management High Availability</b> status window opens.
5	Select <b>Actions &gt; Set Active for the Connected Domain</b> .
6	Close SmartConsole.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the R7x Security Management Server, Export the entire management database**

Step	Instructions
1	Connect to the command line on the R7x Security Management Server.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	Export the entire management database:  <pre>yes   nohup ./migrate export [-f] [-n] /&lt;Full Path&gt;/&lt;Name of R7x MgmtServer Exported File&gt;</pre> For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate</i> .
6	Calculate the MD5 for the exported database file:  <pre>md5sum /&lt;Full Path&gt;/&lt;Name of R7x MgmtServer Exported File&gt;.tgz</pre>
7	Transfer the exported database from the R7x Standalone to an external storage:  <pre>/&lt;Full Path&gt;/&lt;Name of R7x MgmtServer Exported File&gt;.tgz</pre>   <b>Note</b> - Make sure to transfer the file in the binary mode.

### 3. On the R80.40 Multi-Domain Server, create a new Domain Management Server

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in to the Expert mode.
3	<p>Create a new Domain Management Server:</p>  <b>Note</b> - This is one long command with multiple parameters. <pre>mgmt_cli --root true add domain name &lt;Name of New Domain&gt; comments "&lt;Desired Comment Text&gt;" servers.ip-address &lt;IPv4 Address of New Domain&gt; servers.name &lt;Name of New Domain Management Server&gt; servers.multi-domain-server &lt;Name of R80.40 Multi-Domain Server&gt; servers.skip-start-domain- server true</pre> <p>For more information, see the <a href="#">Check Point Management API Reference</a> - <code>mgmt_cli</code> tool - Chapter <i>Multi-Domain</i> - Section <i>Domain</i> - Subsection <i>add domain</i>.</p>  <b>Important</b> - After you create the new Domain with this command, do <b>not</b> change the Domain IPv4 address until you run the " <code>cma_migrate</code> " command.

### 4. Transfer the exported R7x Security Management Server management database to the R80.40 Multi-Domain Server

Step	Instructions
1	Transfer the exported R7x Security Management Server management database from an external storage to the R80.40 Multi-Domain Server, to some directory.
2	 <b>Note</b> - Make sure to transfer the file in the binary mode.  <p>Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the R7x Standalone:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of R7x MgmtServer Exported File&gt;.tgz</pre>

### 5. On the R80.40 Multi-Domain Server, import R7x Security Management Server management database to the new Domain Management Server

Step	Instructions
1	<p>Unset the shell idle environment variable:</p> <pre>unset TMOUT</pre>
2	<p>Import the R7x Security Management Server management database:</p> <pre>cma_migrate &lt;Full Path&gt;/&lt;Name of R7x StandAlone Exported File&gt;.tgz &lt;Full Path&gt;/&lt;\$FWDIR Directory of the New Domain Management Server&gt;/</pre> <p>Example:</p> <pre>cma_migrate /var/log/orig_R7x_database.tgz /opt/CPmds-R80.40/customers/MyDomain3/CPSuite-R80.40/fw1/</pre> <p> <b>Note</b> - This command updates the database schema before it imports. First, the command runs pre-upgrade verification. If no errors are found, migration continues. If there are errors, you must fix them on the source R7x Security Management Server according to instructions in the error messages. Then do this procedure again.</p>

## 6. Reset SIC, create a new ICA, and establish SIC Trust with managed Security Gateways

**Important:**



- This step applies if the new R80.40 Domain Management Server has a different IPv4 address than the R7x Security Management Server.
- In a Cluster, you must configure all the Cluster Members in the same way.

When a Management Server and a managed Security Gateway establish SIC Trust, the Security Gateway saves the IP address of the Internal Certificate Authority (ICA) of its Management Server. The Security Gateway uses this IP address for Automatic Certificate Renewal process when the certificate on the Security Gateway expires.

To force the Security Gateway to update the saved IP address of the Management Server's ICA, follow *one* of these procedures:

### Reset and establish SIC Trust again (recommended)

**Warning:**



- In Cluster, this procedure can cause a failover.
- Until Check Point processes restart, traffic does not pass through the Security Gateway (Cluster Member).

For more information, see [sk65764: How to reset SIC](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Start the Check Point Configuration Tool. Run:

```
cpconfig
```

- c. Choose the option **Secure Internal Communication** from the menu - enter 5 press the Enter key.  
Follow the instructions on the screen to re-initialize the communication and to enter the Activation Key.
- d. Exit the Check Point Configuration Tool.
- e. Wait for Check Point processes to restart.
- f. Connect with SmartConsole to the Management Server that manages the Security Gateway (Cluster) object.
- g. From the left navigation panel, click **Gateways & Servers**.
- h. Double-click the Security Gateway (Cluster) object.
- i. From the left tree, click **General Properties**.  
In a Cluster object, click **Cluster Members** and edit every Cluster Member object.
- j. Click **Communication**.
- k. Click **Reset**.
- l. Enter the same Activation Key you entered on the Security Gateway (Cluster Member).
- m. Click **Initialize**.
- n. The **Trust State** field must show **Trust established**.
- o. Click **Close**.
- p. Click **OK**.
- q. Publish the SmartConsole session.
- r. Install the Access Control Policy on the Security Gateway (Cluster) object.

### **Manually update the saved ICA IP address on the Security Gateway**

For more information, see [sk103356: How to renew SIC after changing IP Address of Security Management Server](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Log in to the Expert mode.
- c. Back up the current \$CPDIR/registry/HKLM\_registry.data file:  

```
cp -v $CPDIR/registry/HKLM_registry.data{,_BKP}
```
- d. Edit the current \$CPDIR/registry/HKLM\_registry.data file:  

```
vi $CPDIR/registry/HKLM_registry.data
```

- e. Search for:

```
:ICAip
```

Example of the applicable section:

```
: (SIC
  :ICAdn ("O=R80.40-Manager..ntk6rk")
  :MySICname ("CN=R80.40-MyGW,O=R80.40-Manager..ntk6rk")
  :HasCertificate ("[4]1")
  :CertPath ("/opt/CPshrd-R80.40/conf/sic_cert.p12")
  :ICAip (192.168.41.80)
```

- f. Change the value of the ":ICAip" to the new IP address.

- g. Save the changes in the file and exit the editor.

## 7. Configure the VPN keys



**Important** - This step applies if the original R7x Security Management Server managed VPN gateways.

There can be an issue with the IKE certificates after you migrate the management database, if a VPN tunnel is established between a Check Point Security Gateway and an externally managed, third-party gateway.

The VPN Security Gateway presents its IKE certificate to its peer.

The third-party gateway uses the FQDN of the certificate to retrieve the host name and IP address of the Certificate Authority.

If the IKE certificate was issued by a Check Point Internal CA, then the FQDN contains the host name of the original Management Server.

The peer gateway will fail to contact the original server and will not accept the certificate.

To fix:

- Update the external DNS server to resolve the host name to the IP address of the applicable Domain Management Server.
- Revoke the IKE certificate for the Security Gateway and create a new one.

# Migrating Database from an R7x Domain Management Server to an R80.40 Domain Management Server

This procedure lets you export the entire management database from a specific Domain Management Server on an R7x Multi-Domain Server and import it to a new Domain Management Server on an R80.40 Multi-Domain Server.



**Note** - This procedure is **not** supported for exporting the management database from a specific Domain Management Server on an R8x Multi-Domain Server and importing it on an R80.40 Multi-Domain Server.

**Important** - Before you migrate a database:

Step	Instructions
1	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27). <b>The procedure below resets SIC on the Domain Management Server to be migrated!</b>
2	Make sure in R7x SmartDomain Manager that there is one Domain Management Server in the Active state in each Domain to be migrated.
3	Make sure that you are migrating the database only on one Domain Management Server. If you migrate a database to more than one Domain Management Server, the import fails and shows an error message.



**Important** - Before you import the database on the Secondary Multi-Domain Server in Management High Availability, you must change the state of its Global Domain to **Active**.

## Instructions

Step	Instructions
1	Connect with SmartConsole to the Secondary Multi-Domain Server.
2	From the left navigation panel, click <b>Multi Domain &gt; Domains</b> .
3	Right-click the Global Domain of the Secondary Multi-Domain Server and click <b>Connect to Domain</b> . A window shows for the Global Domain.
4	Click <b>Menu &gt; Management High Availability</b> . The <b>Management High Availability</b> status window opens.
5	Select <b>Actions &gt; Set Active for the Connected Domain</b> .
6	Close SmartConsole.

**Procedure:****1. Get the R80.40 Management Server Migration Tool**

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on page 182).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

**2. On the R7x Multi-Domain Server, export the Domain Management Server management database**

Step	Instructions
1	Connect to the command line on the R7x Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Go to the directory, where you put the R80.40 Management Server Migration Tool package:  <pre>cd /var/log/path_to_migration_tool/</pre>
5	Extract the R80.40 Management Server Migration Tool package:  <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
6	Go to the context of the applicable Domain Management Server:  <pre>mdsenv &lt;IP Address or Name of Domain Management Server&gt;</pre>
7	Export the entire management database from the Domain Management Server:  <pre>yes   nohup ./migrate export [-l   -x] /&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;</pre> For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate</i> .
8	Calculate the MD5 for the exported database file:  <pre>md5sum /&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz</pre>

Step	Instructions
9	<p>Transfer the exported Domain Management Server database from the current Multi-Domain Server to an external storage:</p> <pre>/&lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

### 3. On the R80.40 Multi-Domain Server, create a new Domain Management Server

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Create a new Domain Management Server:</p> <p> <b>Note</b> - This is one long command with multiple parameters.</p> <pre>mgmt_cli --root true add domain name &lt;Name of New Domain&gt; comments "&lt;Desired Comment Text&gt;" servers.ip-address &lt;IPv4 Address of New Domain&gt; servers.name &lt;Name of New Domain Management Server&gt; servers.multi-domain-server &lt;Name of R80.40 Multi-Domain Server&gt; servers.skip-start-domain-server true</pre> <p>For more information, see the <a href="#">Check Point Management API Reference</a> - mgmt_cli tool - Chapter Multi-Domain - Section Domain - Subsection add domain.</p> <p> <b>Important</b> - xxx</p> <p><b>Important</b> - After you create the new Domain with this command, do <b>not</b> change the Domain IPv4 address until you run the "cma_migrate" command.</p>

### 4. Transfer the exported R7x Domain Management Server management database to the R80.40 Multi-Domain Server

Step	Instructions
1	<p>Transfer the exported R7x Domain Management Server management database from an external storage to the R80.40 Multi-Domain Server, to some directory.</p> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

Step	Instructions
2	<p>Make sure the transferred file is not corrupted.</p> <p>Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the R7x Multi-Domain Server:</p> <pre>md5sum &lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz</pre>

5. **On the R80.40 Multi-Domain Server, import the R7x Domain Management Server management database to the new Domain Management Server**

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	<p>Unset the shell idle environment variable:</p> <pre>unset TMOUT</pre>
5	<p>Import the R7x Domain Management Server management database:</p> <pre>cma_migrate &lt;Full Path&gt;/&lt;Name of R7x Domain Exported File&gt;.tgz &lt;Full Path&gt;/&lt;\$FWDIR Directory of the New Domain Management Server&gt;/</pre> <p><b>Example:</b></p> <pre>cma_migrate /var/log/orig_R7x_database.tgz /opt/CPmds-R80.40/customers/MyDomain3/CPsuite-R80.40/fw1/</pre> <p> <b>Note</b> - This command updates the database schema before it imports. First, the command runs pre-upgrade verification. If no errors are found, migration continues. If there are errors, you must fix them on the source R7x Domain Management Server according to instructions in the error messages. Then do this procedure again.</p>
6	<p>Start the new Domain Management Server with the imported R7x management database:</p> <pre>mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt;</pre>

Step	Instructions
7	<p>All the required daemons (FWM, FWD, CPD, and CPC) on the new Domain Management Server must be in the state "up" and show their PID:</p> <pre>mdsstat</pre> <p>If some of the required daemons on a Domain Management Server are in the state "down" or "N/A" even after for 5-10 minutes, then restart that Domain Management Server, and check again:</p> <pre>mdsstopp_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstart_customer &lt;IP Address or Name of Domain Management Server&gt; mdsstat</pre>

## 6. Reset SIC, create a new ICA, and establish SIC Trust with managed Security Gateways



**Important:**

- This step applies if the new R80.40 Domain Management Server has a different IPv4 address than the R7x Domain Management Server.
- In a Cluster, you must configure all the Cluster Members in the same way.

When a Management Server and a managed Security Gateway establish SIC Trust, the Security Gateway saves the IP address of the Internal Certificate Authority (ICA) of its Management Server. The Security Gateway uses this IP address for Automatic Certificate Renewal process when the certificate on the Security Gateway expires.

To force the Security Gateway to update the saved IP address of the Management Server's ICA, follow *one* of these procedures:

### Reset and establish SIC Trust again (recommended)



**Warning:**

- In Cluster, this procedure can cause a failover.
- Until Check Point processes restart, traffic does not pass through the Security Gateway (Cluster Member).

For more information, see [sk65764: How to reset SIC](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Start the Check Point Configuration Tool. Run:

```
cpconfig
```

- c. Choose the option **Secure Internal Communication** from the menu - enter 5 press the Enter key.

Follow the instructions on the screen to re-initialize the communication and to enter the Activation Key.

- d. Exit the Check Point Configuration Tool.
- e. Wait for Check Point processes to restart.

- f. Connect with SmartConsole to the Management Server that manages the Security Gateway (Cluster) object.
- g. From the left navigation panel, click **Gateways & Servers**.
- h. Double-click the Security Gateway (Cluster) object.
- i. From the left tree, click **General Properties**.  
In a Cluster object, click **Cluster Members** and edit every Cluster Member object.
- j. Click **Communication**.
- k. Click **Reset**.
- l. Enter the same Activation Key you entered on the Security Gateway (Cluster Member).
- m. Click **Initialize**.
- n. The **Trust State** field must show **Trust established**.
- o. Click **Close**.
- p. Click **OK**.
- q. Publish the SmartConsole session.
- r. Install the Access Control Policy on the Security Gateway (Cluster) object.

### **Manually update the saved ICA IP address on the Security Gateway**

For more information, see [sk103356: How to renew SIC after changing IP Address of Security Management Server](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Log in to the Expert mode.
- c. Back up the current \$CPDIR/registry/HKLM\_registry.data file:

```
cp -v $CPDIR/registry/HKLM_registry.data{,_BKP}
```

- d. Edit the current \$CPDIR/registry/HKLM\_registry.data file:

```
vi $CPDIR/registry/HKLM_registry.data
```

- e. Search for:

```
:ICAip
```

Example of the applicable section:

<pre>: (SIC     :ICAdn ("O=R80.40-Manager..ntk6rk")     :MySICname ("CN=R80.40-MyGW,O=R80.40-Manager..ntk6rk")     :HasCertificate ("[4]1")     :CertPath ("/opt/CPShrd-R80.40/conf/sic_cert.p12")     :ICAip (192.168.41.80)</pre>
---

- f. Change the value of the ":ICAip" to the new IP address.
- g. Save the changes in the file and exit the editor.

## 7. Configure the VPN keys



**Important** - This step applies if the original R7x Domain Management Server managed VPN gateways.

There can be an issue with the IKE certificates after you migrate the management database, if a VPN tunnel is established between a Check Point Security Gateway and an externally managed, third-party gateway.

The VPN Security Gateway presents its IKE certificate to its peer.

The third-party gateway uses the FQDN of the certificate to retrieve the host name and IP address of the Certificate Authority.

If the IKE certificate was issued by a Check Point Internal CA, then the FQDN contains the host name of the original Management Server.

The peer gateway will fail to contact the original server and will not accept the certificate.

To fix:

- Update the external DNS server to resolve the host name to the IP address of the applicable Domain Management Server.
- Revoke the IKE certificate for the Security Gateway and create a new one.

## Procedure to migrate a management database from R7x Domain Management Server on a Secondary R80.40 Multi-Domain Server

Step	Instructions
1	Connect to the command line on the Secondary R80.40 Multi-Domain Server.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Connect with SmartConsole to the Secondary Multi-Domain Server.
5	From the left navigation panel, click <b>Multi Domain &gt; Domains</b> .
6	Right-click the Global Domain of the Secondary Multi-Domain Server and click <b>Connect to Domain</b> .
7	In the top left corner, click <b>Menu &gt; Management High Availability</b> .
8	In the <b>High Availability Status</b> window, in the <b>Connected To</b> section, click <b>Actions &gt; Set Active</b> .
9	Close the Domain SmartConsole instance.

# Migrating Database from an R7x Standalone to an R80.40 Domain Management Server

Migration from a Standalone to a Domain Management Server is supported only from R7x versions to a Domain Management Server on a Multi-Domain Server R80.20 or higher.

To do this, you have to separate the Security Management Server and Security Gateway on the R7x Standalone. Then you manage the former Standalone as a Security Gateway only, from the R80.40 Domain Management Server.

**Important** - Before you migrate the database:



Step	Instructions
1	Make sure that the target Domain Management Server can communicate with all the Security Gateways managed by the R7x Standalone.
2	Back up your current configuration (see " <a href="#">Backing Up and Restoring</a> " on page 27).

**Procedure:**

1. Configure the required policies to allow communication with R80.40 Domain Management Server

Step	Instructions
1	Connect with R7x SmartDashboard to the R7x Standalone.
2	<p>Create a new <b>Check Point Host</b> object to represent the R80.40 Domain Management Server and define it as a <b>Secondary Security Management Server</b>.</p> <ol style="list-style-type: none"> <li>a. Create the object in one of these ways: <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New</b> ( &gt; More &gt; Check Point Host.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways &amp; Servers</b> &gt; <b>New Check Point Host</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Check Point Host</b>.</li> </ul> </li> <li>b. In the <b>Name</b> field, enter the applicable name.</li> <li>c. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, enter the applicable IP addresses of the R80.40 Domain Management Server.</li> <li>d. In the <b>Platform</b> section: <ul style="list-style-type: none"> <li>■ In the <b>Hardware</b> field, select the applicable option</li> <li>■ In the <b>Version</b> field, select the highest version.</li> <li>■ In the <b>OS</b> field, select <b>Gaia</b></li> </ul> </li> <li>e. Do not initialize the SIC communication.</li> <li>f. On the <b>General Properties</b> page, click the <b>Management</b> tab. Make sure the <b>Secondary Server</b> is selected and grayed out.</li> <li>g. Click <b>OK</b>.</li> </ol>

Step	Instructions
3	Create the applicable <b>Firewall</b> rules in all applicable policies to allow the new <b>Check Point Host</b> object (that represents the R80.40 Domain Management Server) to communicate with all managed Security Gateways.
4	Install the <b>Network Security</b> policies on all managed Security Gateways.
5	Delete the new <b>Check Point Host</b> object (that represents the R80.40 Domain Management Server) and the <b>Firewall</b> rules created in <b>Steps 2 - 4</b> .
6	Save the changes (click <b>File &gt; Save</b> ).

## 2. Configure the R7x Standalone object

Step	Instructions
1	If the R7x Standalone object participates in a VPN community, remove it from the VPN community and delete its certificate. Note these settings, to configure them again after the migration.
2	Remove the R7x Standalone object from the <b>Install On</b> column in all policies.
3	Open the R7x Standalone object.
4	Click <b>General Properties</b> page > <b>Network Security</b> tab.
5	Clear <b>all</b> the Software Blades.
6	Click <b>OK</b> .
7	Save the changes (click <b>File &gt; Save</b> ).
8	Do <b>not</b> install the <b>Network Security</b> policy on the R7x Standalone object.
9	Close the SmartDashboard.

## 3. Get the R80.40 Management Server Migration Tool

Step	Instructions
1	Download the R80.40 Management Server Migration Tool from the <a href="#">R80.40 Home Page SK</a> (see " <i>Management Server Migration Tool and Upgrade Tools</i> " on <a href="#">page 182</a> ).
2	Transfer the R80.40 Management Server Migration Tool package to the current server to some directory (for example, /var/log/path_to_migration_tool/).   <b>Note</b> - Make sure to transfer the file in the binary mode.

## 4. On the R7x Standalone, Export the entire management database

Step	Instructions
1	Connect to the command line on the R7x Standalone.
2	Log in to the Expert mode.
3	Go to the directory, where you put the R80.40 Management Server Migration Tool package: <pre>cd /var/log/path_to_migration_tool/</pre>
4	Extract the R80.40 Management Server Migration Tool package: <pre>tar zxvf &lt;Name of Management Server Migration Tool Package&gt;.tgz</pre>
5	Export the entire management database: <pre>yes   nohup ./migrate export [-f] [-n] /&lt;Full Path&gt;/&lt;Name of R7x StandAlone Exported File&gt;</pre> <p>For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>migrate</i>.</p>
6	Calculate the MD5 for the exported database file: <pre>md5sum /&lt;Full Path&gt;/&lt;Name of R7x StandAlone Exported File&gt;.tgz</pre>
7	Transfer the exported database from the R7x Standalone to an external storage: <pre>/&lt;Full Path&gt;/&lt;Name of R7x StandAlone Exported File&gt;.tgz</pre> <p> <b>Note</b> - Make sure to transfer the file in the binary mode.</p>

## 5. On the R80.40 Multi-Domain Server, create a new Domain Management Server

Step	Instructions
1	Connect to the command line on the R80.40 Multi-Domain Server.
2	Log in to the Expert mode.

Step	Instructions
3	<p>Create a new Domain Management Server:</p>  <p><b>Note</b> - This is one long command with multiple parameters.</p> <pre>mgmt_cli --root true add domain name &lt;Name of New Domain&gt; comments "&lt;Desired Comment Text&gt;" servers.ip-address &lt;IPv4 Address of New Domain&gt; servers.name &lt;Name of New Domain Management Server&gt; servers.multi-domain-server &lt;Name of R80.40 Multi-Domain Server&gt; servers.skip-start-domain- server true</pre> <p>For more information, see the <a href="#">Check Point Management API Reference</a> - <code>mgmt_cli</code> tool - Chapter <i>Multi-Domain</i> - Section <i>Domain</i> - Subsection <i>add domain</i>.</p>  <p><b>Important</b> - After you create the new Domain with this command, do <b>not</b> change the Domain IPv4 address until you run the "<code>cma_migrate</code>" command.</p>

## 6. Transfer the exported R7x Standalone management database to the R80.40 Multi-Domain Server

Step	Instructions
1	<p>Transfer the exported R7x Standalone management database from an external storage to the R80.40 Multi-Domain Server, to some directory.</p>  <p><b>Note</b> - Make sure to transfer the file in the binary mode.</p>
2	<p>Make sure the transferred file is not corrupted. Calculate the MD5 for the transferred file and compare it to the MD5 that you calculated on the R7x Standalone:</p> <pre>md5sum /&lt;Full Path&gt;/&lt;Name of R7x StandAlone Exported File&gt;.tgz</pre>

## 7. On the R80.40 Multi-Domain Server, import R7x Standalone management database to the new Domain Management Server

Step	Instructions
1	<p>Unset the shell idle environment variable:</p> <pre>unset TMOUT</pre>

Step	Instructions
2	<p>Import the R7x Standalone management database:</p> <pre>cma_migrate /&lt;Full Path&gt;/&lt;Name of R7x StandAlone Exported File&gt;.tgz /&lt;Full Path&gt;/&lt;\$FWDIR Directory of the New Domain Management Server&gt;/</pre> <p>Example:</p> <pre>cma_migrate /var/log/orig_R7x_database.tgz /opt/CPmds-R80.40 /customers/MyDomain3/CPsuite-R80.40/fw1/</pre> <p> <b>Note</b> - This command updates the database schema before it imports. First, the command runs pre-upgrade verification. If no errors are found, migration continues. If there are errors, you must fix them on the source R7x Standalone according to instructions in the error messages. Then do this procedure again.</p>

## 8. Update the ICA IP address on the managed Security Gateways

### Important:



- This step applies if the new R80.40 Domain Management Server has a different IPv4 address than the source R7x Standalone.
- In a Cluster, you must configure all the Cluster Members in the same way.

When a Management Server and a managed Security Gateway establish SIC Trust, the Security Gateway saves the IP address of the Internal Certificate Authority (ICA) of its Management Server. The Security Gateway uses this IP address for Automatic Certificate Renewal process when the certificate on the Security Gateway expires.

To force the Security Gateway to update the saved IP address of the Management Server's ICA, follow *one* of these procedures:

### Reset and establish SIC Trust again (recommended)

#### Warning:



- In Cluster, this procedure can cause a failover.
- Until Check Point processes restart, traffic does not pass through the Security Gateway (Cluster Member).

For more information, see [sk65764: How to reset SIC](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Start the Check Point Configuration Tool. Run:

```
cpconfig
```

- c. Choose the option **Secure Internal Communication** from the menu - enter 5 press the Enter key.  
Follow the instructions on the screen to re-initialize the communication and to enter the Activation Key.
- d. Exit the Check Point Configuration Tool.
- e. Wait for Check Point processes to restart.
- f. Connect with SmartConsole to the Management Server that manages the Security Gateway (Cluster) object.
- g. From the left navigation panel, click **Gateways & Servers**.
- h. Double-click the Security Gateway (Cluster) object.
- i. From the left tree, click **General Properties**.  
In a Cluster object, click **Cluster Members** and edit every Cluster Member object.
- j. Click **Communication**.
- k. Click **Reset**.
- l. Enter the same Activation Key you entered on the Security Gateway (Cluster Member).
- m. Click **Initialize**.
- n. The **Trust State** field must show **Trust established**.
- o. Click **Close**.
- p. Click **OK**.
- q. Publish the SmartConsole session.
- r. Install the Access Control Policy on the Security Gateway (Cluster) object.

### **Manually update the saved ICA IP address on the Security Gateway**

For more information, see [sk103356: How to renew SIC after changing IP Address of Security Management Server](#).

- a. Connect to the command line on the Security Gateway (every Cluster Member).
- b. Log in to the Expert mode.
- c. Back up the current \$CPDIR/registry/HKLM\_registry.data file:  

```
cp -v $CPDIR/registry/HKLM_registry.data{,_BKP}
```
- d. Edit the current \$CPDIR/registry/HKLM\_registry.data file:  

```
vi $CPDIR/registry/HKLM_registry.data
```

- e. Search for:

```
:ICAip
```

Example of the applicable section:

```
: (SIC
  :ICAdn ("O=R80.40-Manager..ntk6rk")
  :MySICname ("CN=R80.40-MyGW,O=R80.40-Manager..ntk6rk")
  :HasCertificate ("[4]1")
  :CertPath ("/opt/CPshrd-R80.40/conf/sic_cert.p12")
  :ICAip (192.168.41.80)
```

- f. Change the value of the ":ICAip" to the new IP address.

- g. Save the changes in the file and exit the editor.

## 9. Configure the VPN keys



**Important** - This step applies if the original R7x Standalone managed VPN gateways.

There can be an issue with the IKE certificates after you migrate the management database, if a VPN tunnel is established between a Check Point Security Gateway and an externally managed, third-party gateway.

The VPN Security Gateway presents its IKE certificate to its peer.

The third-party gateway uses the FQDN of the certificate to retrieve the host name and IP address of the Certificate Authority.

If the IKE certificate was issued by a Check Point Internal CA, then the FQDN contains the host name of the original Management Server.

The peer gateway will fail to contact the original server and will not accept the certificate.

To fix:

- Update the external DNS server to resolve the host name to the IP address of the applicable Domain Management Server.
- Revoke the IKE certificate for the Security Gateway and create a new one.

## 10. Configure the Domain Management Server object in SmartConsole

The Domain Management Server object represents the Management Server component of the R7x Standalone.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Domain Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	<p>Locate these objects:</p> <ul style="list-style-type: none"> <li>■ An object with the Name and IP address of the Domain Management Server.</li> <li>Previous references to the R7x Standalone object now refer to this object.</li> <li>■ An object for each Security Gateway managed previously by the R7x Standalone.</li> </ul>
4	Open the Domain Management Server object.
5	From the left navigation tree, click <b>Network Management</b> .
6	<p>Delete all interfaces:</p> <ol style="list-style-type: none"> <li>a. Select each interface.</li> <li>b. Click <b>Actions &gt; Delete Interface</b>.</li> <li>c. Click <b>Yes</b>.</li> </ol>
7	Click <b>OK</b> .
8	Publish the SmartConsole session.

## 11. Create the new Security Gateway object in SmartConsole

You must create a new Security Gateway object to represent the Gateway component of the R7x Standalone.

This new Security Gateway object represents the separate Security Gateway.

Step	Instructions
1	Connect with SmartConsole to the R80.40 Domain Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new Security Gateway object (that represents the Gateway component of the R7x Standalone) in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object &gt; Gateways and Servers &gt; New Gateway</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Gateway</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>. <b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
5	In the <b>Name</b> field, enter the applicable name for this Security Gateway object.
6	In the <b>IPv4 address</b> (and <b>IPv6 address</b> ) field, enter some dummy IP address. Later, you change this IP address to the real IP address.
7	Do <b>not</b> establish the Secure Internal Communication.

Step	Instructions
8	In the <b>Platform</b> section, select the correct options: <ol style="list-style-type: none"> <li>In the <b>Hardware</b> field:               <ul style="list-style-type: none"> <li>■ If you install the Security Gateway on a Check Point Appliance, select the correct appliances series.</li> <li>■ If you install the Security Gateway on an Open Server, select <b>Open server</b>.</li> </ul> </li> <li>In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
9	On the <b>General Properties</b> page: <ul style="list-style-type: none"> <li>■ On the <b>Network Security</b> tab, enable the applicable Software Blades.</li> <li>■ On the <b>Threat Prevention</b> tab, enable the applicable Software Blades.</li> </ul>
10	Click <b>OK</b> .
11	Publish the SmartConsole session.

## 12. Install the R80.40 Security Gateway

You must install a separate Security Gateway to represent the Gateway component of the R7x Standalone.

You can install the Security Gateway from scratch on the former R7x Standalone server.

Step	Instructions
A	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
B	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
C	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster</b>, type.</li> </ol> </li> <li>■ In the <b>Dynamically Assigned IP</b> window, select the <b>No</b>.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

## 13. Configure the new Security Gateway object in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the new R80.40 Domain Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	Open the Security Gateway object that represents the Gateway component of the R7x Standalone.
4	<p>In the <b>IPv4 address</b> and <b>IPv6 address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Gateway's First Time Configuration Wizard.</p> <p>Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p>
5	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:</p> <ol style="list-style-type: none"> <li>Near the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>In the <b>Platform</b> field: <ul style="list-style-type: none"> <li>Select <b>Open server / Appliance</b> for all Check Point models 3000 and higher.</li> <li>Select <b>Open server / Appliance</b> for an Open Server.</li> </ul> </li> <li>Enter the same <b>Activation Key</b> you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>OK</b>.</li> </ol>
	<p>If the <b>Certificate state</b> field does not show <b>Established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Gateway.</li> <li>Make sure there is a physical connectivity between the Security Gateway and the Management Server (for example, pings can pass).</li> <li>Run:  <pre>cpcfg</pre> </li> <li>Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpcfg</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
6	Click <b>OK</b> .
7	Publish the SmartConsole session.

#### 14. Replace the R7x Standalone object in all policies in SmartConsole

You must create a new Security Gateway object to represent the Gateway component of the R7x Standalone.

This new Security Gateway object represents the separate Security Gateway.

Step	Instructions
1	Connect with SmartConsole to the new R80.40 Domain Management Server.

Step	Instructions
2	From the left navigation panel, click <b>Security Policies</b> .
3	In all existing policies, replace the R7x Standalone object with the new Security Gateway object that represents the Gateway component of the R7x Standalone.
4	Publish the SmartConsole session.
5	Install the Access Control Policy on all applicable Security Gateways.
5	Install the Threat Prevention Policy on all applicable Security Gateways.

# Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server

This procedure lets you change the current IP Address of a Multi-Domain Server or Multi-Domain Log Server.



**Note** - In environments with multiple Multi-Domain Servers or Multi-Domain Log Servers, perform the procedure for each applicable Multi-Domain Server or Multi-Domain Log Server.

## Procedure:

1. **Back up the current R80.40 Multi-Domain Server or Multi-Domain Log Server**

See "[Backing Up and Restoring](#)" on page 27.

2. **Change the IP address on the applicable interface**



**Note** - This step applies only if it is necessary to use the same physical interface, but with a different IP address.

See the [R80.40 Gaia Administration Guide](#) > Chapter Network Management > Section Network Interfaces > Section Physical Interfaces.

3. **Install the new license for the new IP address**

Step	Instructions
1	Connect to your <a href="#">Check Point User Center</a> account.
2	Issue a new license for the new IP address of your Multi-Domain Server or Multi-Domain Log Server.
3	Get the new license and Support Contract.
4	Install the new license and Support Contract in the MDS context on your Multi-Domain Server or Multi-Domain Log Server. See " <a href="#">Working with Licenses</a> " on page 791.

4. **Connect to the command line on the Multi-Domain Server or Multi-Domain Log Server**

Step	Instructions
1	Connect over SSH, or serial console.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.

Step	Instructions
4	Go to the MDS context: <pre>mdsenv</pre>

## 5. Stop all processes in the MDS context

Step	Instructions
1	Stop all processes in the MDS context: <pre>mdsstop -m</pre>  <b>Important</b> - While these process are stopped, SmartConsole cannot connect.
2	Make sure all processes stopped in the MDS context: <pre>mdsstat -m</pre> All the daemons (FWM, FWD, CPD, and CPC) must be in the state "down".

## 6. Change the IP address in the MDS database



**Important** - This step applies *only* if the MDS object already exists in the database.

For example, this step does **not** apply to a new Secondary Multi-Domain Server or Multi-Domain Log Server in a clean installation.

Step	Instructions
1	Change the IP address: <pre>\$MDSDIR/bin/mdscmd change-mds-ip &lt;Current IP Address&gt; &lt;New IP Address&gt; ipv4 -x</pre> Example: <pre>\$MDSDIR/bin/mdscmd change-mds-ip 192.168.20.30 172.30.40.50 ipv4 -x</pre>

Step	Instructions
2	<p>Make sure the IP address is updated in the <b>dleobjectderef_data</b> database:</p> <ol style="list-style-type: none"> <li>Save the applicable data from this database to a file:</li> </ol> <pre>psql_client -c "select fwset from dleobjectderef_data where cpmitable='mdss' and not deleted and dlesession=0" -o /tmp/dleobject.txt cpm postgres</pre> <ol style="list-style-type: none"> <li>Examine the IP address:</li> </ol> <pre>cat /tmp/dleobject.txt   egrep -w 'name ipaddr'</pre> <p>Example output:</p> <pre>:name (My_MDS_Server) :ipaddr (172.30.40.50)</pre>
3	<p>Make sure the IP address is updated in the <b>cplnetworkobject_data</b> database:</p> <ol style="list-style-type: none"> <li>Save the applicable data from this database to a file:</li> </ol> <pre>psql_client -c "select name, ipaddress4 from cplnetworkobject_data where not deleted and dlesession=0" -o /tmp/cplnetworkobject.txt cpm postgres</pre> <ol style="list-style-type: none"> <li>Examine the IP address:</li> </ol> <pre>cat /tmp/cplnetworkobject.txt</pre> <p>Example output:</p> <pre>name   ipaddress4 -----+----- My_MDS_Server   172.30.40.50</pre>

## 7. Modify the \$MDSDIR/conf/external.if file

**Important:**



- This step applies if you change the Leading Interface to another physical interface.
- This step applies if you migrated the entire management database from a source Multi-Domain Server or Multi-Domain Log Server to a target Multi-Domain Server or Multi-Domain Log Server, and the target server uses a different external interface (for example, `eth0` on the source server and `eth1` on the target server).

Step	Instructions
1	<p>Back up the current \$MDSDIR/conf/external.if file:</p> <pre>cp -v \$MDSDIR/conf/external.if{,_BKP}</pre>
2	<p>Edit the current \$MDSDIR/conf/external.if file:</p> <pre>vi \$MDSDIR/conf/external.if</pre>

Step	Instructions
3	Change the current interface name to the name of the applicable main interface. This is the interface, on which you configured the main IPv4 address of your Multi-Domain Server or Multi-Domain Log Server.
4	Save the changes and exit the Vi editor.
5	Go to the context of each existing Domain Management Server: <pre>mdsenv &lt;IP Address or Name of Domain Management Server&gt;</pre>
6	Back up the current \$FWDIR/conf/vip_index.conf file: <pre>cp -v \$FWDIR/conf/vip_index.conf{,_BKP}</pre>
7	Edit the current \$FWDIR/conf/vip_index.conf file: <pre>vi \$FWDIR/conf/vip_index.conf</pre>
8	Change the current interface name to the name of the applicable main interface. This is the interface, on which you configured the main IPv4 address of your Multi-Domain Server or Multi-Domain Log Server.
9	Save the changes and exit the Vi editor.

#### 8. Modify the \$MDSDIR/conf/LeadingIP file

Step	Instructions
1	Back up the current \$MDSDIR/conf/LeadingIP file: <pre>cp -v \$MDSDIR/conf/LeadingIP{,_BKP}</pre>
2	Edit the current file: <pre>vi \$MDSDIR/conf/LeadingIP</pre>
3	Change the current IP address to the new IP address.
4	Save the changes in the file and exit the editor.

#### 9. Modify the \$MDSDIR/conf/mdsdb/mdss.C file

Step	Instructions
1	Back up the current \$MDSDIR/conf/mdsdb/mdss.C file: <pre>cp -v \$MDSDIR/conf/mdsdb/mdss.C{,_BKP}</pre>
2	Edit the current \$MDSDIR/conf/mdsdb/mdss.C file: <pre>vi \$MDSDIR/conf/mdsdb/mdss.C</pre>

Step	Instructions
3	Find the object of your Multi-Domain Server or Multi-Domain Log Server that has the current IP address.
4	Change the object's IP address to the new IP address.
5	Do <b>not</b> change the object's name.
6	Save the changes in the file and exit the editor.

#### 10. Modify the `$SMARTLOGDIR/smartlog_settings.txt` file

Step	Instructions
1	Back up the current <code>\$SMARTLOGDIR/smartlog_settings.txt</code> file: <pre>cp -v \$SMARTLOGDIR/smartlog_settings.txt{,_BKP}</pre>
2	Edit the current file: <pre>vi \$SMARTLOGDIR/smartlog_settings.txt</pre>
3	Change the current IP address to the new IP address in these parameters: <ul style="list-style-type: none"> <li>■ Parameter :server_port ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :management &gt; Parameter :name ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :log_servers &gt; Parameter :name ()</li> </ul>
4	Save the changes in the file and exit the editor.

#### 11. Modify the `$INDEXERDIR/log_indexer_custom_settings.conf` file

Step	Instructions
1	Back up the current <code>\$INDEXERDIR/log_indexer_custom_settings.conf</code> file: <pre>cp -v \$INDEXERDIR/log_indexer_custom_settings.conf{,_BKP}</pre>
2	Edit the current file: <pre>vi \$INDEXERDIR/log_indexer_custom_settings.conf</pre>
3	Change the current IP address to the new IP address in these parameters: <ul style="list-style-type: none"> <li>■ Parameter :server_port ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :management &gt; Parameter :name ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :log_servers &gt; Parameter :name ()</li> </ul>
4	Save the changes in the file and exit the editor.

## 12. Start all processes in the MDS context

Step	Instructions
1	<p>Start all processes in the MDS context:</p> <pre>mdsstart -m</pre>
2	<p>Make sure all processes started in the MDS context:</p> <pre>mdsstat -m</pre> <p>All the daemons (FWM, FWD, CPD, and CPC) must be in the state "up" and show their PID.</p>

## 13. Change the IP addresses of all existing Domain Management Servers and Domain Log Servers

Follow "["Changing the IP Address of a Domain Management Server or Domain Log Server" on page 687.](#)

### Important Notes

- If you just installed the *Secondary* Multi-Domain Server or Multi-Domain Log Server, and it is necessary to change the server's IP address, you only need to change the \$MDSDIR/conf/LeadingIP file.
- After you change the IP address of the Multi-Domain Server or Multi-Domain Log Server, you have to synchronize the local log database again on these servers (see [sk116335](#)):



**Important** - Perform this synchronization only after you change the IP addresses of all existing Domain Management Servers and Domain Log Servers.

- Multi-Domain Server
- Secondary Multi-Domain Server (if it is installed in the environment)
- Multi-Domain Log Server
- Secondary Multi-Domain Log Server (if it is installed in the environment)
- Global SmartEvent Server (if it is installed in the environment)

# Changing the IP Address of a Domain Management Server or Domain Log Server

This procedure lets you change the current IP Address of:

- A Domain Management Server on a Multi-Domain Server
- A Domain Log Server on a Multi-Domain Log Server

**Important:**



- See "[Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server](#)" on page 681.
- On Multi-Domain Servers in a Management High Availability environment, you must perform the procedure below in this order:
  1. Change the IP address on the *Active* Domain Management Server on the *Primary* Multi-Domain Server
  2. On the *Primary* Multi-Domain Server, change the state of the *Active* Domain Management Server to *Standby*
  3. On the *Secondary* Multi-Domain Server, change the state of the applicable Domain Management Server to *Active*
  4. Change the IP address on the *Active* Domain Management Server on the *Secondary* Multi-Domain Server
- On Multi-Domain Log Servers in a Management High Availability environment, you must perform the procedure below in this order:
  1. Change the IP address on the *Active* Domain Log Server on the *Primary* Multi-Domain Log Server
  2. On the *Primary* Multi-Domain Log Server, change the state of the *Active* Domain Log Server to *Standby*
  3. On the *Secondary* Multi-Domain Log Server, change the state of the applicable Domain Log Server to *Active*
  4. Change the IP address on the *Active* Domain Log Server on the *Secondary* Multi-Domain Log Server

**Procedure:**

1. **Back up the current R80.40 Multi-Domain Server or Multi-Domain Log Server**

See "[Backing Up and Restoring](#)" on page 27.

2. **Close all SmartConsole applications**

You must close all GUI clients (SmartConsole applications) connected to the Multi-Domain Server or Multi-Domain Log Server.

3. **Connect to the command line on the Multi-Domain Server or Multi-Domain Log Server**

Step	Instructions
1	Connect over SSH, or serial console.

Step	Instructions
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Go to the MDS context: mdsenv

#### 4. Stop the applicable Domain Management Server or Domain Log Server

Step	Instructions
1	Stop the services: <code>mdsstop_customer &lt;Name or IP of Domain Management Server or Domain Log Server&gt;</code>
2	Make sure the services stopped in the applicable context: <code>mdsstat</code> All the daemons (FWM, FWD, CPD, and CPC) must be in the state "down".

#### 5. Change the IP address in the MDS database

Step	Instructions
1	<p>Change the IP address:</p> <pre>\$MDS_TEMPLATE/scripts/change_cma_ip.sh -n &lt;Name of Domain Management Server or Domain Log Server object&gt; -i &lt;New IP Address&gt;</pre> <p>Example:</p> <pre>\$MDS_TEMPLATE/scripts/change_cma_ip.sh -n My_Domain_Server -i 172.30.40.55</pre> <p>You can change the IP addresses of several Domain Management Servers or Domain Log Servers in one command:</p> <ol style="list-style-type: none"> <li>Make sure the services stopped in all applicable contexts.</li> <li>Create a plain text file that contains pairs of server names and their new IPv4 addresses (separated with comma).</li> </ol> <p>Example of a file:</p> <pre>MyDomainManagementServer_1, 172.30.40.51 MyDomainManagementServer_2, 172.30.40.52 MyDomainManagementServer_3, 172.30.40.53</pre> <p>c. Run this command:</p> <pre>\$MDS_TEMPLATE/scripts/change_cma_ip.sh -f /&lt;Path To&gt;/&lt;File&gt;</pre>

#### 6. Modify the \$SMARTLOGDIR/smartlog\_settings.txt file

Step	Instructions
1	<p>Go to the context of the Domain Management Server or Domain Log Server:</p> <pre>mdsenv &lt;Name or IP of Domain Management Server or Domain Log Server&gt;</pre>
2	<p>Back up the current \$SMARTLOGDIR/smartlog_settings.txt file:</p> <pre>cp -v \$SMARTLOGDIR/smartlog_settings.txt{,_BKP}</pre>
3	<p>Edit the current file:</p> <pre>vi \$SMARTLOGDIR/smartlog_settings.txt</pre>
4	<p>Change the current IP address to the new IP address in these parameters:</p> <ul style="list-style-type: none"> <li>■ Parameter :server_port ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :management &gt; Parameter :name ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :log_servers &gt; Parameter :name ()</li> </ul>
5	Save the changes in the file and exit the editor.

## 7. Modify the \$INDEXERDIR/log\_indexer\_custom\_settings.conf file

Step	Instructions
1	<p>Go to the context of the Domain Management Server or Domain Log Server:</p> <pre>mdsenv &lt;Name or IP of Domain Management Server or Domain Log Server&gt;</pre>
2	<p>Back up the current \$INDEXERDIR/log_indexer_custom_settings.conf file:</p> <pre>cp -v \$INDEXERDIR/log_indexer_custom_settings.conf{,_BKP}</pre>
3	<p>Edit the current file:</p> <pre>vi \$INDEXERDIR/log_indexer_custom_settings.conf</pre>
4	<p>Change the current IP address to the new IP address in these parameters:</p> <ul style="list-style-type: none"> <li>■ Parameter :server_port ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :management &gt; Parameter :name ()</li> <li>■ Section :connections &gt; Section :domain &gt; Section :log_servers &gt; Parameter :name ()</li> </ul>
5	Save the changes in the file and exit the editor.

## 8. Start the applicable Domain Management Server or Domain Log Server

Step	Instructions
1	<p>Start the services:</p> <pre data-bbox="433 276 1410 339">mdsstart_customer &lt;Name or IP of Domain Management Server or Domain Log Server&gt;</pre>
2	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPC) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="433 478 560 505">mdsstat</pre> <p>If some of the required daemons on a Domain Management Server (Domain Log Server) are in the state "down", then wait for 5-10 minutes, restart that Domain Management Server (Domain Log Server), and check again. Run these three commands:</p> <pre data-bbox="433 680 1338 842">mdsstopp_customer &lt;IP Address or Name or IP of Domain Management Server or Domain Log Server&gt; mdsstart_customer &lt;IP Address or Name or IP of Domain Management Server or Domain Log Server&gt; mdsstat</pre>

### Important Note

If SmartLog does not work for a Domain Management Server with the modified IP address:

1. Connect with SmartConsole to that Domain Management Server.
2. From the left navigation panel, click **Gateways & Servers**.
3. Open the Domain Management Server object.
4. Make any change in the Domain Management Server object (for example, in the **Comment** field).
5. Click **OK**.
6. Publish the SmartConsole session.

# IPS in Multi-Domain Server Environment

When you upgrade a Multi-Domain Server from R7x to R80.40, the previous Domain IPS configuration is overridden when you first assign a Global Policy.

## Notes:



- If you manage IPS globally, you must reassign the Global Policies before installing the policy on the managed Security Gateways.
- Starting in R80, the IPS subscription has changed. All Domains subscribed to IPS, are automatically assigned to an "Exclusive" subscription. "Override" and "Merge" subscriptions are no longer supported.
- For more on IPS in Multi-Domain Server environment, see the [R80.40 Multi-Domain Security Management Administration Guide](#).

# Special Scenarios for Security Gateways

This section describes special scenarios for Security Gateways:

- [\*"Deploying a Security Gateway in Monitor Mode" on page 693\*](#)
- [\*"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726\*](#)
- [\*"Security Before Firewall Activation" on page 783\*](#)

# Deploying a Security Gateway in Monitor Mode

## Introduction to Monitor Mode

You can configure Monitor Mode on a single Check Point Security Gateway's interface.

The Check Point Security Gateway 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 Gateway with an interface configured in Monitor Mode to record the activity logs.

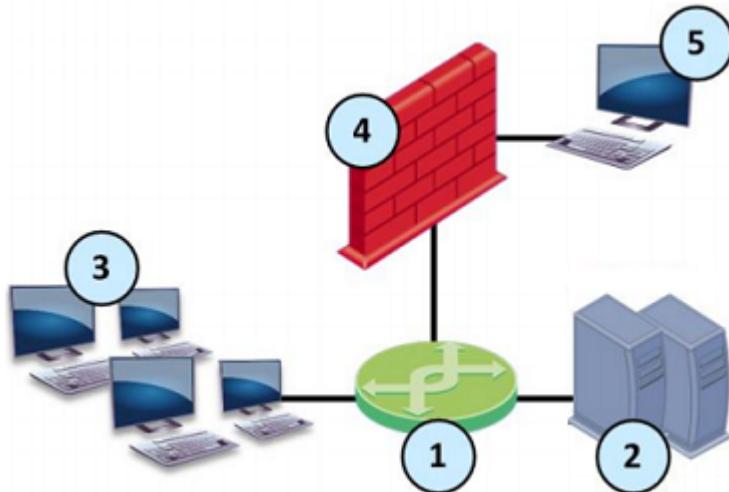
### You can use the Monitor Mode:

- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Software Blades:
  - The Security Gateway neither enforces any security policy, nor performs any active operations (prevent / drop / reject) on the interface in the Monitor Mode.
  - The Security Gateway terminates and does not forward all packets that arrive at the interface in the Monitor Mode.
  - The Security Gateway 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 Gateway connects to a mirror or SPAN port on the switch.
2	Servers.
3	Clients.
4	Security Gateway with an interface in Monitor Mode.
5	Security Management Server that manages the Security Gateway.

## Supported Software Blades in Monitor Mode

This table lists Software Blades and their support for the Monitor Mode in a single Security Gateway deployment.



**Important** - Check Point Cluster does not support the Monitor Mode.

Software Blade	Support for the Monitor Mode
Firewall	Fully supports the Monitor Mode.
IPS	These protections and features do <b>not</b> work: <ul style="list-style-type: none"> <li>■ The <b>SYN Attack</b> protection (SYNDefender).</li> <li>■ The <b>Initial Sequence Number (ISN) Spoofing</b> protection.</li> <li>■ The <b>Send error page</b> action in Web Intelligence protections.</li> <li>■ Client and Server notifications about connection termination.</li> </ul>
Application Control	Does <b>not</b> support UserCheck.

Software Blade	Support for the Monitor Mode
URL Filtering	Does <b>not</b> support UserCheck.
Data Loss Prevention	<p>Does <b>not</b> support these:</p> <ul style="list-style-type: none"> <li>■ UserCheck.</li> <li>■ The "<b>Prevent</b>" and "<b>Ask User</b>" actions - these are automatically demoted to the "<b>Inform User</b>" action.</li> <li>■ FTP inspection.</li> </ul>
Identity Awareness	<p>Does <b>not</b> support these:</p> <ul style="list-style-type: none"> <li>■ Captive Portal.</li> <li>■ Identity Agent.</li> </ul>
Threat Emulation	<p>Does <b>not</b> support these:</p> <ul style="list-style-type: none"> <li>■ The Emulation Connection Prevent Handling Modes "<b>Background</b>" and "<b>Hold</b>". See <a href="#">sk106119</a>.</li> <li>■ FTP inspection.</li> </ul>
Content Awareness	Does <b>not</b> support the FTP inspection.
Anti-Bot	Fully supports the Monitor Mode.
Anti-Virus	Does <b>not</b> support the FTP inspection.
IPsec VPN	Does <b>not</b> support the Monitor Mode.
Mobile Access	Does <b>not</b> support the Monitor Mode.
Anti-Spam & Email Security	Does <b>not</b> support the Monitor Mode.
QoS	Does <b>not</b> support the Monitor Mode.

# Limitations in Monitor Mode

These features and deployments are **not** supported in Monitor Mode:

- Passing production traffic through a Security Gateway, on which you configured Monitor Mode interface(s).
- If you configure more than one Monitor Mode interface on a Security Gateway, you must make sure the Security Gateway does not receive the same traffic on the different Monitor Mode interfaces.
- HTTPS Inspection
- NAT rules.
- HTTP / HTTPS proxy.
- Anti-Virus in Traditional Mode.
- User Authentication.
- Client Authentication.
- Check Point Active Streaming (CPAS).
- Cluster deployment.
- CloudGuard Gateways.
- CoreXL Dynamic Dispatcher ([sk105261](#)).
- Setting the value of the kernel parameters "psl\_tap\_enable" and "fw\_tap\_enable" to 1 (one) on-the-fly with the "fw ctl set int" command (Issue ID 02386641).

For more information, see [sk101670: Monitor Mode on Gaia OS and SecurePlatform OS](#).

# Configuring a Single Security Gateway in Monitor Mode

**Important:**



- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the Security Gateway in Monitor Mode to the Internet.
- You must install valid license and contracts file on the Security Gateway in Monitor Mode.



**Note** - This procedure applies to both Check Point Appliances and Open Servers.

**Procedure:**

1. **Install the Security Gateway**

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Management Connection</b> window, select the interface, through which you connect to Gaia operating system.</li> <li>■ In the <b>Internet Connection</b> window, do not configure IP addresses.</li> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster</b>, type.</li> </ol> </li> <li>■ In the <b>Dynamically Assigned IP</b> window, select <b>No</b>.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

2. **Configure the Monitor Mode on the applicable interface**

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia Clish.

**Configuring the Monitor Mode in Gaia Portal**

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <code>https://&lt;IP address of Gaia Management Interface&gt;</code> </div>
2	In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b> .

Step	Instructions
3	Select the applicable physical interface from the list and click <b>Edit</b> .
4	Select the <b>Enable</b> option to set the interface status to UP.
5	In the <b>Comment</b> field, enter the applicable comment text (up to 100 characters).
6	On the <b>IPv4</b> tab, select <b>Use the following IPv4 address</b> , but do not enter an IPv4 address.
7	On the <b>IPv6</b> tab, select <b>Use the following IPv6 address</b> , but do not enter an IPv6 address.
	 <b>Important</b> - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the <b>Ethernet</b> tab: <ul style="list-style-type: none"> <li>■ Select <b>Auto Negotiation</b>, or select a link speed and duplex setting from the list.</li> <li>■ In the <b>Hardware Address</b> field, enter the Hardware MAC address (if not automatically received from the NIC).          <b>Caution</b> - Do not manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure.       </li> <li>■ In the <b>MTU</b> field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500).</li> <li>■ Select <b>Monitor Mode</b>.</li> </ul>
9	Click <b>OK</b> .

### Configuring the Monitor Mode in Gaia Clish

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to Gaia Clish.
3	Examine the configuration and state of the applicable physical interface: <pre data-bbox="462 1664 1203 1697">show interface &lt;Name of Physical Interface&gt;</pre>

Step	Instructions
4	<p>If the applicable physical interface has an IP address assigned to it, remove that IP address.</p> <ul style="list-style-type: none"> <li>■ To remove an IPv4 address:</li> </ul> <pre data-bbox="536 339 1430 406">delete interface &lt;Name of Physical Interface&gt; ipv4-address</pre> <ul style="list-style-type: none"> <li>■ To remove an IPv6 address:</li> </ul> <pre data-bbox="536 473 1430 541">delete interface &lt;Name of Physical Interface&gt; ipv6-address</pre>
5	<p>Enable the Monitor Mode on the physical interface:</p> <pre data-bbox="477 631 1410 698">set interface &lt;Name of Physical Interface&gt; monitor-mode on</pre>
6	<p>Configure other applicable settings on the interface in the Monitor Mode:</p> <pre data-bbox="477 788 1256 855">set interface &lt;Name of Physical Interface&gt; ...</pre>
7	<p>Examine the configuration and state of the Monitor Mode interface:</p> <pre data-bbox="477 923 1208 990">show interface &lt;Name of Physical Interface&gt;</pre>
8	<p>Save the configuration:</p> <pre data-bbox="477 1057 668 1102">save config</pre>

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

You can configure the Security Gateway object in SmartConsole either in Wizard Mode, or in Classic Mode.

#### Configuring the Security Gateway object in Wizard Mode

Step	Instructions
1	<p>Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Gateway.</p>
2	<p>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</p>
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★) &gt; Gateway</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>New Gateway</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Gateway</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Wizard Mode</b>.</p>

Step	Instructions
5	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Gateway name</b> field, enter the applicable name for this Security Gateway object.</li> <li>In the <b>Gateway platform</b> field, select the correct hardware type.</li> <li>In the <b>Gateway IP address</b> section, select <b>Static IP address</b> and configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Gateway's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> <li>Click <b>Next</b>.</li> </ol>
6	<p>On the <b>Trusted Communication</b> page:</p> <ol style="list-style-type: none"> <li>Select the applicable option: <ul style="list-style-type: none"> <li>If you selected <b>Initiate trusted communication now</b>, enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>If you selected <b>Skip and initiate trusted communication later</b>, make sure to follow Step 7.</li> </ul> </li> <li>Click <b>Next</b>.</li> </ol>
7	<p>On the <b>End</b> page:</p> <ol style="list-style-type: none"> <li>Examine the <b>Configuration Summary</b>.</li> <li>Select <b>Edit Gateway properties for further configuration</b>.</li> <li>Click <b>Finish</b>.</li> </ol> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
8	<p>If during the Wizard Mode, you selected <b>Skip and initiate trusted communication later</b>:</p> <ol style="list-style-type: none"> <li>The <b>Secure Internal Communication</b> field shows <b>Uninitialized</b>.</li> <li>Click <b>Communication</b>.</li> <li>In the <b>Platform</b> field: <ul style="list-style-type: none"> <li>Select <b>Open server / Appliance</b> for all Check Point models 3000 and higher.</li> <li>Select <b>Open server / Appliance</b> for an Open Server.</li> </ul> </li> <li>Enter the same <b>Activation Key</b> you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>. Make sure the <b>Certificate state</b> field shows <b>Established</b>.</li> <li>Click <b>OK</b>.</li> </ol>
9	<p>On the <b>Network Security</b> tab, make sure to enable only the Firewall Software Blade.</p>
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Get Interfaces &gt; Get Interfaces With Topology</b>.</li> <li>Confirm the interfaces information.</li> </ol>

Step	Instructions
11	<p>Select the interface in the Monitor Mode and click <b>Edit</b>. Configure these settings:</p> <ol style="list-style-type: none"> <li>a. Click the <b>General</b> page.</li> <li>b. In the <b>General</b> section, enter a <i>random</i> IPv4 address.</li> </ol> <p> <b>Important</b> - This random IPv4 address must not conflict with existing IPv4 addresses on your network.</p> <ol style="list-style-type: none"> <li>c. In the <b>Topology</b> section: Click <b>Modify</b>. In the <b>Leads To</b> section, select <b>Not defined (Internal)</b>. In the <b>Security Zone</b> section, select <b>According to topology: Internal Zone</b>. Click <b>OK</b> to close the <b>Topology Settings</b> window.</li> <li>d. Click <b>OK</b> to close the <b>Interface</b> window.</li> </ol>
12	Click <b>OK</b> .
13	Publish the SmartConsole session.
14	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 Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>New Gateway</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Gateway</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>. <b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
5	In the <b>Name</b> field, enter the applicable name for this Security Gateway object.
6	<p>In the <b>IPv4 address</b> and <b>IPv6 address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Gateway's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p>

Step	Instructions
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:</p> <ol style="list-style-type: none"> <li>Near the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>In the <b>Platform</b> field: <ul style="list-style-type: none"> <li>■ Select <b>Open server / Appliance</b> for all Check Point models 3000 and higher.</li> <li>■ Select <b>Open server / Appliance</b> for an Open Server.</li> </ul> </li> <li>Enter the same <b>Activation Key</b> you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>OK</b>.</li> </ol>
	<p>If the <b>Certificate state</b> field does not show <b>Established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Gateway.</li> <li>Make sure there is a physical connectivity between the Security Gateway and the Management Server (for example, pings can pass).</li> <li>Run:  <pre>cpconfig</pre> </li> <li>Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
8	<p>In the <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>In the <b>Hardware</b> field: <ul style="list-style-type: none"> <li>■ If you install the Security Gateway on a Check Point Appliance, select the correct appliances series.</li> <li>■ If you install the Security Gateway on an Open Server, select <b>Open server</b>.</li> </ul> </li> <li>In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
9	<p>On the <b>Network Security</b> tab, make sure to enable only the Firewall Software Blade.</p> <p> <b>Important - Do not select anything on the Management tab.</b></p>
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Get Interfaces &gt; Get Interfaces With Topology</b>.</li> <li>Confirm the interfaces information.</li> </ol>

Step	Instructions
11	<p>Select the interface in the Monitor Mode and click <b>Edit</b>. Configure these settings:</p> <ul style="list-style-type: none"> <li>a. Click the <b>General</b> page.</li> <li>b. In the <b>General</b> section, enter a <i>random</i> IPv4 address.</li> </ul> <p> <b>Important</b> - This random IPv4 address must not conflict with existing IPv4 addresses on your network.</p> <ul style="list-style-type: none"> <li>c. In the <b>Topology</b> section: Click <b>Modify</b>. In the <b>Leads To</b> section, select <b>Not defined (Internal)</b>. In the <b>Security Zone</b> section, select <b>According to topology: Internal Zone</b>. Click <b>OK</b> to close the <b>Topology Settings</b> window.</li> <li>d. Click <b>OK</b> to close the <b>Interface</b> window.</li> </ul>
12	Click <b>OK</b> .
13	Publish the SmartConsole session.
14	This Security Gateway object is now ready to receive the Security Policy.

#### 4. Configure the Security Gateway to process packets that arrive in the wrong order

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.

Step	Instructions
3	<p>Modify the \$FWDIR/boot/modules/fw kern.conf file:</p> <ol style="list-style-type: none"> <li>Back up the current \$FWDIR/boot/modules/fw kern.conf file:</li> </ol> <pre data-bbox="520 354 1197 413">cp -v \$FWDIR/boot/modules/fw kern.conf{,_BKP}</pre> <p>If this file does not exist, create it:</p> <pre data-bbox="520 480 1149 512">touch \$FWDIR/boot/modules/fw kern.conf</pre> <ol style="list-style-type: none"> <li>Edit the current \$FWDIR/boot/modules/fw kern.conf file:</li> </ol> <pre data-bbox="520 579 1097 610">vi \$FWDIR/boot/modules/fw kern.conf</pre> <p> <b>Important</b> - This configuration file does <b>not</b> support spaces or comments.</p> <ol style="list-style-type: none"> <li>Add this line to enable the Passive Streaming Layer (PSL) Tap Mode:</li> </ol> <pre data-bbox="520 855 790 887">psl_tap_enable=1</pre> <ol style="list-style-type: none"> <li>Add this line to enable the Firewall Tap Mode:</li> </ol> <pre data-bbox="520 954 774 985">fw_tap_enable=1</pre> <ol style="list-style-type: none"> <li>Save the changes in the file and exit the Vi editor.</li> </ol>
4	<p>Modify the \$PPKDIR/conf/simkern.conf file:</p> <ol style="list-style-type: none"> <li>Back up the current \$PPKDIR/conf/simkern.conf file:</li> </ol> <pre data-bbox="520 1163 1160 1194">cp -v \$PPKDIR/conf/simkern.conf{,_BKP}</pre> <p>If this file does not exist, create it:</p> <pre data-bbox="520 1262 1049 1293">touch \$PPKDIR/conf/simkern.conf</pre> <ol style="list-style-type: none"> <li>Edit the current \$PPKDIR/conf/simkern.conf file:</li> </ol> <pre data-bbox="520 1361 997 1392">vi \$PPKDIR/conf/simkern.conf</pre> <p> <b>Important</b> - This configuration file does <b>not</b> support spaces or comments.</p> <ol style="list-style-type: none"> <li>Add this line to enable the Firewall Tap Mode:</li> </ol> <pre data-bbox="520 1596 774 1628">fw_tap_enable=1</pre> <ol style="list-style-type: none"> <li>Save the changes in the file and exit the Vi editor.</li> </ol>
5	Reboot the Security Gateway.

Step	Instructions
6	<p>Make sure the Security Gateway loaded the new configuration:</p> <ol style="list-style-type: none"> <li>Examine the status of the PSL Tap Mode:  <pre>fw ctl get int psl_tap_enable</pre> <p>Output must show:  <code>psl_tap_enable = 1</code></p> </li> <li>Examine the status of the Firewall Tap Mode:  <pre>fw ctl get int fw_tap_enable</pre> <p>Output must show:  <code>fw_tap_enable = 1</code></p> </li> </ol>

**Notes:**

- This configuration helps the Security Gateway process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the Security Gateway 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 Gateway 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 "fw ctl set int <parameter>" command (Known Limitation 02386641).

## 5. Configure the required Global Properties for the Security Gateway in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Target Domain Management Server</i> that manages this Security Gateway.
2	In the top left corner, click <b>Menu &gt; Global properties</b> .
3	<p>From the left tree, click the <b>Stateful Inspection</b> pane and configure:</p> <ol style="list-style-type: none"> <li>In the <b>Default Session Timeouts</b> section:           <ol style="list-style-type: none"> <li>Change the value of the <b>TCP session timeout</b> from the default <b>3600</b> to <b>60</b> seconds.</li> <li>Change the value of the <b>TCP end timeout</b> from the default <b>20</b> to <b>5</b> seconds.</li> </ol> </li> <li>In the <b>Out of state packets</b> section, you must clear all the boxes. Otherwise, the Security Gateway drops the traffic as out of state (because the traffic does not pass through the Security Gateway, it does not record the state information for the traffic).</li> </ol>

Step	Instructions
4	From the left tree, click the <b>Advanced</b> page > click the <b>Configure</b> button, and configure: a. Click <b>FireWall-1 &gt; Stateful Inspection</b> . b. Clear <b>reject_x11_in_any</b> . c. Click <b>OK</b> to close the <b>Advanced Configuration</b> window.
5	Click <b>OK</b> to close the <b>Global Properties</b> window.
6	Publish the SmartConsole session.

#### 6. Configure the required Access Control Policy for the Security Gateway in SmartConsole

Step	Instructions																		
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Gateway.																		
2	From the left navigation panel, click <b>Security Policies</b> .																		
3	Create a new policy and configure the applicable layers: a. At the top, click the <b>+</b> tab (or press the <b>CTRL T</b> keys). b. On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b> . c. In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers. d. Click <b>Close</b> . e. On the <b>Manage Policies</b> tab, click the new policy you created.																		
4	Create the <b>Access Control</b> rule that accepts all traffic: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Accept All</td> <td>*Any</td> <td>*Any</td> <td>Any</td> <td>*Any</td> <td>Accept</td> <td>Log</td> <td>Object of Security Gateway in Monitor Mode</td> </tr> </tbody> </table>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install	1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install											
1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode											

Step	Instructions
5	 <b>Best Practice</b> <p>We recommend these <b>Aggressive Aging</b> settings for the most common TCP connections:</p> <ol style="list-style-type: none"> <li>a. In the SmartConsole, click <b>Objects</b> menu &gt; <b>Object Explorer</b>.</li> <li>b. Open <b>Services</b> and select <b>TCP</b>.</li> <li>c. Search for the most common TCP connections in this network.</li> <li>d. Double-click the applicable TCP service.</li> <li>e. From the left tree, click <b>Advanced</b>.</li> <li>f. At the top, select <b>Override default settings</b>. On Domain Management Server, select <b>Override global domain settings</b>.</li> <li>g. Select <b>Match for 'Any'</b>.</li> <li>h. In the <b>Aggressive aging</b> section: Select <b>Enable aggressive aging</b>. Select <b>Specific</b> and enter <b>60</b>.</li> <li>i. Click <b>OK</b>.</li> <li>j. Close the <b>Object Explorer</b>.</li> </ol>
6	Publish the SmartConsole session.
7	Install the Access Control Policy on the Security Gateway object.

## 7. Make sure the Security Gateway enabled the Monitor Mode for Software Blades

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	Install the default policy on the VSX Gateway object: Make sure the parameter <b>fw_span_port_mode</b> is part of the installed policy: <pre data-bbox="414 1462 1346 1507">grep -A 3 -r fw_span_port_mode \$FWDIR/state/local/*</pre> The returned output must show: <pre data-bbox="414 1529 1346 1596">:val (true)</pre>

## 8. Connect the Security Gateway to the switch

On the Security Gateway, connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- [R80.40 Gaia Administration Guide](#).
- [R80.40 Security Management Administration Guide](#).

# Configuring a Single VSX Gateway in Monitor Mode

**Important:**



- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the VSX Gateway in Monitor Mode to the Internet (also, see [sk79700](#) and [sk106496](#)).
- You must install valid license and contracts file on the VSX Gateway in Monitor Mode.



**Note** - This procedure applies to both Check Point Appliances and Open Servers.

**Procedure:**

1. **Install the VSX Gateway**



**Important** - Make sure the VSX Gateway has enough physical interfaces.

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Management Connection</b> window, select the interface, through which you connect to Gaia operating system.</li> <li>■ In the <b>Internet Connection</b> window, do not configure IP addresses.</li> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster, type</b>.</li> </ol> </li> <li>■ In the <b>Dynamically Assigned IP</b> window, select <b>No</b>.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

2. **Configure the Monitor Mode on the applicable interface**

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia Clish.

## Configuring the Monitor Mode in Gaia Portal

Step	Instructions
1	<p>With a web browser, connect to Gaia Portal at:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>https://&lt;IP address of Gaia Management Interface&gt;</code> </div>
2	In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b> .
3	Select the applicable physical interface from the list and click <b>Edit</b> .
4	Select the <b>Enable</b> option to set the interface status to UP.
5	In the <b>Comment</b> field, enter the applicable comment text (up to 100 characters).
6	On the <b>IPv4</b> tab, select <b>Use the following IPv4 address</b> , but do not enter an IPv4 address.
7	On the <b>IPv6</b> tab, select <b>Use the following IPv6 address</b> , but do not enter an IPv6 address.
	 <b>Important</b> - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	<p>On the <b>Ethernet</b> tab:</p> <ul style="list-style-type: none"> <li>■ Select <b>Auto Negotiation</b>, or select a link speed and duplex setting from the list.</li> <li>■ In the <b>Hardware Address</b> field, enter the Hardware MAC address (if not automatically received from the NIC).</li> </ul> <div style="margin-left: 40px;">  <b>Caution</b> - Do not manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure.       </div> <ul style="list-style-type: none"> <li>■ In the <b>MTU</b> field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500).</li> <li>■ Select <b>Monitor Mode</b>.</li> </ul>
9	Click <b>OK</b> .

## Configuring the Monitor Mode in Gaia Clish

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to Gaia Clish.
3	<p>Examine the configuration and state of the applicable physical interface:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>show interface &lt;Name of Physical Interface&gt;</code> </div>

Step	Instructions
4	<p>If the applicable physical interface has an IP address assigned to it, remove that IP address.</p> <ul style="list-style-type: none"> <li>■ To remove an IPv4 address:</li> </ul> <pre data-bbox="536 339 1426 406">delete interface &lt;Name of Physical Interface&gt; ipv4-address</pre> <ul style="list-style-type: none"> <li>■ To remove an IPv6 address:</li> </ul> <pre data-bbox="536 473 1426 541">delete interface &lt;Name of Physical Interface&gt; ipv6-address</pre>
5	<p>Enable the Monitor Mode on the physical interface:</p> <pre data-bbox="473 646 1410 714">set interface &lt;Name of Physical Interface&gt; monitor-mode on</pre>
6	<p>Configure other applicable settings on the interface in the Monitor Mode:</p> <pre data-bbox="473 810 1251 844">set interface &lt;Name of Physical Interface&gt; ...</pre>
7	<p>Examine the configuration and state of the Monitor Mode interface:</p> <pre data-bbox="473 938 1203 972">show interface &lt;Name of Physical Interface&gt;</pre>
8	<p>Save the configuration:</p> <pre data-bbox="473 1066 663 1098">save config</pre>

### 3. Configure the VSX Gateway to process packets that arrive in the wrong order

Step	Instructions
1	Connect to the command line on the VSX Gateway.
2	Log in to the Expert mode.

Step	Instructions
3	<p>Modify the \$FWDIR/boot/modules/fw kern.conf file:</p> <ol style="list-style-type: none"> <li>Back up the current \$FWDIR/boot/modules/fw kern.conf file:  <pre>cp -v \$FWDIR/boot/modules/fw kern.conf{,_BKP}</pre> </li> <li>If this file does not exist, create it:  <pre>touch \$FWDIR/boot/modules/fw kern.conf</pre> </li> <li>Edit the current \$FWDIR/boot/modules/fw kern.conf file:  <pre>vi \$FWDIR/boot/modules/fw kern.conf</pre> </li> </ol> <p> <b>Important</b> - This configuration file does <b>not</b> support spaces or comments.</p> <ol style="list-style-type: none"> <li>Add this line to enable the Passive Streaming Layer (PSL) Tap Mode:  <pre>psl_tap_enable=1</pre> </li> <li>Add this line to enable the Firewall Tap Mode:  <pre>fw_tap_enable=1</pre> </li> <li>Save the changes in the file and exit the Vi editor.</li> </ol>
4	<p>Modify the \$PPKDIR/conf/simkern.conf file:</p> <ol style="list-style-type: none"> <li>Back up the current \$PPKDIR/conf/simkern.conf file:  <pre>cp -v \$PPKDIR/conf/simkern.conf{,_BKP}</pre> </li> <li>If this file does not exist, create it:  <pre>touch \$PPKDIR/conf/simkern.conf</pre> </li> <li>Edit the current \$PPKDIR/conf/simkern.conf file:  <pre>vi \$PPKDIR/conf/simkern.conf</pre> </li> </ol> <p> <b>Important</b> - This configuration file does <b>not</b> support spaces or comments.</p> <ol style="list-style-type: none"> <li>Add this line to enable the Firewall Tap Mode:  <pre>fw_tap_enable=1</pre> </li> <li>Save the changes in the file and exit the Vi editor.</li> </ol>
5	<p>Reboot the VSX Gateway.</p>

Step	Instructions
6	<p>Make sure the VSX Gateway loaded the new configuration:</p> <ol style="list-style-type: none"> <li>Examine the status of the PSL Tap Mode:  <pre>fw ctl get int psl_tap_enable</pre> <p>Output must show:  <code>psl_tap_enable = 1</code></p> </li> <li>Examine the status of the Firewall Tap Mode:  <pre>fw ctl get int fw_tap_enable</pre> <p>Output must show:  <code>fw_tap_enable = 1</code></p> </li> </ol>

**Notes:**

- This configuration helps the VSX Gateway process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the VSX Gateway 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 VSX Gateway 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 "fw ctl set int <parameter>" command (Known Limitation 02386641).

**4. Configure the VSX Gateway object in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Main</i> Domain Management Server that should manage this VSX Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new VSX Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★) &gt; VSX &gt; Gateway</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; VSX &gt; New Gateway</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; VSX &gt; Gateway</b>.</li> </ul> <p>The <b>VSX Gateway Wizard</b> opens.</p>

Step	Instructions
4	<p>On the <b>VSX Gateway General Properties (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Enter the VSX Gateway Name</b> field, enter the applicable name for this VSX Gateway object.</li> <li>In the <b>Enter the VSX Gateway IPv4</b> field, enter the same IPv4 address that you configured on the <b>Management Connection</b> page of the VSX Gateway's First Time Configuration Wizard.</li> <li>In the <b>Enter the VSX Gateway IPv6</b> field, enter the same IPv6 address that you configured on the <b>Management Connection</b> page of the VSX Gateway's First Time Configuration Wizard.</li> <li>In the <b>Select the VSX Gateway Version</b> field, select <b>R80.40</b>.</li> <li>Click <b>Next</b>.</li> </ol>
5	<p>On the <b>VSX Gateway General Properties (Secure Internal Communication)</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Activation Key</b> field, enter the same Activation Key you entered during the VSX Gateway's First Time Configuration Wizard.</li> <li>In the <b>Confirm Activation Key</b> field, enter the same Activation Key again.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>Next</b>.</li> </ol>
	<p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the VSX Gateway.</li> <li>Make sure there is a physical connectivity between the VSX Gateway and the Management Server (for example, pings can pass).</li> <li>Run:  <pre>cpconfig</pre> </li> <li>Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, on the <b>VSX Gateway General Properties</b> page, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
6	<p>On the <b>VSX Gateway Interfaces (Physical Interfaces Usage)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway.</li> <li>If you plan to connect more than one Virtual System directly to the same physical interface, you must select <b>VLAN Trunk</b> for that physical interface.</li> <li>Click <b>Next</b>.</li> </ol>
7	<p>On the <b>Virtual Network Device Configuration (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>You can select <b>Create a Virtual Network Device</b> and configure the first applicable Virtual Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router.</li> <li>Click <b>Next</b>.</li> </ol>

Step	Instructions
8	<p>On the <b>VSX Gateway Management (Specify the management access rules)</b> page:</p> <ol style="list-style-type: none"> <li>a. Examine the default access rules.</li> <li>b. Select the applicable default access rules.</li> <li>c. Configure the applicable source objects, if needed.</li> <li>d. Click <b>Next</b>.</li> </ol>  <p><b>Important</b> - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.</p>
9	<p>On the <b>VSX Gateway Creation Finalization</b> page:</p> <ol style="list-style-type: none"> <li>a. Click <b>Finish</b> and wait for the operation to finish.</li> <li>b. Click <b>View Report</b> for more information.</li> <li>c. Click <b>Close</b>.</li> </ol>
10	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 900 711 934">vsx stat -v</pre>
11	<p>Install the default policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> <li>a. Click <b>Install Policy</b>.</li> <li>b. In the <b>Policy</b> field, select the default policy for this VSX Gateway object. This policy is called:</li> </ol> <div style="border: 1px solid black; padding: 2px; display: inline-block;">&lt;Name of VSX Gateway object&gt;_VSX</div> <ol style="list-style-type: none"> <li>c. Click <b>Install</b>.</li> </ol>
12	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 1417 711 1450">vsx stat -v</pre>

## 5. Configure the Virtual System object (and other Virtual Devices) in SmartConsole

Step	Instructions
1	<p>Connect with SmartConsole to the Security Management Server, or each <i>Target Domain Management Server</i> that should manage each Virtual Device.</p>

Step	Instructions
2	<p>Configure the applicable Virtual System (and other Virtual Devices) on this VSX Gateway.</p> <p>When you configure this Virtual System, for the Monitor Mode interface, add a regular interface. In the <b>IPv4 Configuration</b> section, enter a <i>random</i> IPv4 address.</p>  <p><b>Important</b> - This random IPv4 address must not conflict with existing IPv4 addresses on your network.</p>
3	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the VSX Gateway.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run:</li> </ol> <pre data-bbox="520 698 1446 736">vsx stat -v</pre>
4	<p>Disable the Anti-Spoofing on the interface that is configured in the Monitor Mode:</p> <ol style="list-style-type: none"> <li>a. In the SmartConsole, open the Virtual System object.</li> <li>b. Click the <b>Topology</b> page.</li> <li>c. Select the Monitor Mode interface and click <b>Edit</b>. The <b>Interface Properties</b> window opens.</li> <li>d. Click the <b>General</b> tab.</li> <li>e. In the <b>Security Zone</b> field, select <b>None</b>.</li> <li>f. Click the <b>Topology</b> tab.</li> <li>g. In the <b>Topology</b> section, make sure the settings are <b>Internal (leads to the local network)</b> and <b>Not Defined</b>.</li> <li>h. In the <b>Anti-Spoofing</b> section, clear <b>Perform Anti-Spoofing based on interface topology</b>.</li> <li>i. Click <b>OK</b> to close the <b>Interface Properties</b> window.</li> <li>j. Click <b>OK</b> to close the <b>Virtual System Properties</b> window.</li> <li>k. The Management Server pushes the VSX Configuration.</li> </ol>

## 6. Configure the required Global Properties for the Virtual System in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Target Domain</i> Management Server that manages this Virtual System.
2	In the top left corner, click <b>Menu &gt; Global properties</b> .

Step	Instructions
3	<p>From the left tree, click the <b>Stateful Inspection</b> pane and configure:</p> <ul style="list-style-type: none"> <li>a. In the <b>Default Session Timeouts</b> section:           <ul style="list-style-type: none"> <li>i. Change the value of the <b>TCP session timeout</b> from the default <b>3600</b> to <b>60</b> seconds.</li> <li>ii. Change the value of the <b>TCP end timeout</b> from the default <b>20</b> to <b>5</b> seconds.</li> </ul> </li> <li>b. In the <b>Out of state packets</b> section, you must clear all the boxes. Otherwise, the Virtual System drops the traffic as out of state (because the traffic does not pass through the Virtual System, it does not record the state information for the traffic).</li> </ul>
4	<p>From the left tree, click the <b>Advanced</b> page &gt; click the <b>Configure</b> button, and configure:</p> <ul style="list-style-type: none"> <li>a. Click <b>FireWall-1 &gt; Stateful Inspection</b>.</li> <li>b. Clear <b>reject_x11_in_any</b>.</li> <li>c. Click <b>OK</b> to close the <b>Advanced Configuration</b> window.</li> </ul>
5	Click <b>OK</b> to close the <b>Global Properties</b> window.
6	Publish the SmartConsole session.

## 7. Configure the required Access Control policy for the Virtual System in SmartConsole

Step	Instructions																		
1	Connect with SmartConsole to the Security Management Server or <i>Target Domain</i> Management Server that manages this Virtual System.																		
2	From the left navigation panel, click <b>Security Policies</b> .																		
3	<p>Create a new policy and configure the applicable layers:</p> <ul style="list-style-type: none"> <li>a. At the top, click the <b>+</b> tab (or press the <b>CTRL T</b> keys).</li> <li>b. On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>c. In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>d. Click <b>Close</b>.</li> <li>e. On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ul>																		
4	<p>Create the <b>Access Control</b> rule that accepts all traffic:</p> <table border="1"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Accept All</td> <td>*Any</td> <td>*Any</td> <td>Any</td> <td>*Any</td> <td>Accept</td> <td>Log</td> <td>Object of Virtual System</td> </tr> </tbody> </table>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install	1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Virtual System
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install											
1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Virtual System											

Step	Instructions
5	 <b>Best Practice</b> <p>We recommend these <b>Aggressive Aging</b> settings for the most common TCP connections:</p> <ol style="list-style-type: none"> <li>In the SmartConsole, click <b>Objects</b> menu &gt; <b>Object Explorer</b>.</li> <li>Open <b>Services</b> and select <b>TCP</b>.</li> <li>Search for the most common TCP connections in this network.</li> <li>Double-click the applicable TCP service.</li> <li>From the left tree, click <b>Advanced</b>.</li> <li>At the top, select <b>Override default settings</b>. On Domain Management Server, select <b>Override global domain settings</b>.</li> <li>Select <b>Match for 'Any'</b>.</li> <li>In the <b>Aggressive aging</b> section: <ul style="list-style-type: none"> <li>■ Select <b>Enable aggressive aging</b>.</li> <li>■ Select <b>Specific</b> and enter <b>60</b>.</li> </ul> </li> <li>Click <b>OK</b>.</li> <li>Close the <b>Object Explorer</b>.</li> </ol>
6	Publish the SmartConsole session.
7	Install the Access Control Policy on the Virtual System object. <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable policy for this Virtual System object.</li> <li>Click <b>Install</b>.</li> </ol>
8	Examine the VSX configuration: <ol style="list-style-type: none"> <li>Connect to the command line on the VSX Gateway.</li> <li>Log in to the Expert mode.</li> <li>Run: <pre>vsx stat -v</pre> </li> </ol>

#### 8. Make sure the VSX Gateway enabled the Monitor Mode for Software Blades

Step	Instructions
1	Connect to the command line on the VSX Gateway.
2	Log in to the Expert mode.
3	Install the default policy on the VSX Gateway object: Make sure the parameter <b>fw_span_port_mode</b> is part of the installed policy: <pre>grep -A 3 -r fw_span_port_mode \$FWDIR/state/local/*</pre> The returned output must show: <pre>:val (true)</pre>

## 9. Connect the VSX Gateway to the switch

On the VSX Gateway, connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- [\*R80.40 Gaia Administration Guide\*](#).
- [\*R80.40 VSX Administration Guide\*](#).
- [\*R80.40 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 Gateway in Monitor Mode:

Step	Instructions											
	Protected Scope	Protection/Site/File/Blade	Action	Track								
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Gateway.											
2	From the left navigation panel, click <b>Security Policies &gt; Threat Prevention</b> .											
3	Create the <b>Threat Prevention</b> rule that accepts all traffic:											
	<table border="1"> <thead> <tr> <th>Protected Scope</th><th>Protection/Site/File/Blade</th><th>Action</th><th>Track</th></tr> </thead> <tbody> <tr> <td>*Any</td><td>-- N/A</td><td>Applicable Threat Prevention Profile</td><td>Log Packet Capture</td></tr> </tbody> </table>				Protected Scope	Protection/Site/File/Blade	Action	Track	*Any	-- N/A	Applicable Threat Prevention Profile	Log Packet Capture
Protected Scope	Protection/Site/File/Blade	Action	Track									
*Any	-- N/A	Applicable Threat Prevention Profile	Log Packet Capture									
	<p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ We recommend the <b>Optimized</b> profile.</li> <li>■ The <b>Track</b> setting <b>Packet Capture</b> is optional.</li> </ul>											
4	Right-click the selected Threat Prevention profile and click <b>Edit</b> .											
5	From the left tree, click the <b>General Policy</b> page and configure: <ol style="list-style-type: none"> <li>In the <b>Blades Activation</b> section, select the applicable Software Blades.</li> <li>In the <b>Activation Mode</b> section:               <ul style="list-style-type: none"> <li>■ In the <b>High Confidence</b> field, select <b>Detect</b>.</li> <li>■ In the <b>Medium Confidence</b> field, select <b>Detect</b>.</li> <li>■ In the <b>Low Confidence</b> field, select <b>Detect</b>.</li> </ul> </li> </ol>											
6	From the left tree, click the <b>Anti-Virus</b> page and configure: <ol style="list-style-type: none"> <li>In the <b>Protected Scope</b> section, select <b>Inspect incoming and outgoing files</b>.</li> <li>In the <b>File Types</b> section:               <ul style="list-style-type: none"> <li>■ Select <b>Process all file types</b>.</li> <li>■ <b>Optional:</b> Select <b>Enable deep inspection scanning (impacts performance)</b>.</li> </ul> </li> <li><b>Optional:</b> In the <b>Archives</b> section, select <b>Enable Archive scanning (impacts performance)</b>.</li> </ol>											
7	From the left tree, click the <b>Threat Emulation</b> page > click <b>General</b> and configure: <ul style="list-style-type: none"> <li>■ In the <b>Protected Scope</b> section, select <b>Inspect incoming files from the following interfaces</b> and from the menu, select <b>All</b>.</li> </ul>											
8	Configure other applicable settings for the Software Blades.											
9	Click <b>OK</b> .											
10	Install the Threat Prevention Policy on the Security Gateway object.											

**For more information:**

See the [\*R80.40 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 Gateway in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click <b>Manage &amp; Settings &gt; Blades</b> .
3	In the <b>Application Control &amp; URL Filtering</b> section, click <b>Advanced Settings</b> . The <b>Application Control &amp; URL Filtering Settings</b> window opens.
4	On the <b>General</b> page: <ul style="list-style-type: none"> <li>■ In the <b>Fail mode</b> section, select <b>Allow all requests (fail-open)</b>.</li> <li>■ In the <b>URL Filtering</b> section, select <b>Categorize HTTPS websites</b>.</li> </ul>
5	On the <b>Check Point online web service</b> page: <ul style="list-style-type: none"> <li>■ In the <b>Website categorization mode</b> section, select <b>Background</b>.</li> <li>■ Select <b>Categorize social networking</b> widgets.</li> </ul>
6	Click <b>OK</b> to close the <b>Application Control &amp; URL Filtering Settings</b> window.
7	Install the Access Control Policy on the Security Gateway object.

For more information, see the:

- [R80.40 Security Management Administration Guide](#)
- [R80.40 Next Generation Security Gateway 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 Gateway in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click <b>Manage &amp; Settings &gt; Blades</b> .
3	In the <b>Data Loss Prevention</b> section, click <b>Configure in SmartDashboard</b> . The SmartDashboard window opens.
4	In SmartDashboard: <ol style="list-style-type: none"> <li>Click the <b>My Organization</b> page.</li> <li>In the <b>Email Addresses or Domains</b> section, configure with full list of company's domains. There is no need to include subdomains (for example, mydomain.com, mydomain.uk).</li> <li>In the <b>Networks</b> section, select <b>Anything behind the internal interfaces of my DLP gateways</b>.</li> <li>In the <b>Users</b> section, select <b>All users</b>.</li> </ol>
5	Click the <b>Policy</b> page. Configure the applicable rules: <ul style="list-style-type: none"> <li>In the <b>Data</b> column, right-click the pre-defined data types and select <b>Edit</b>.               <ul style="list-style-type: none"> <li>On the <b>General Properties</b> page, in the <b>Flag</b> field, select <b>Improve Accuracy</b>.</li> <li>In the <b>Customer Names</b> data type, we recommend to add the company's real customer names.</li> </ul> </li> <li>In the <b>Action</b> column, you must select <b>Detect</b>.</li> <li>In the <b>Severity</b> column, select <b>Critical</b> or <b>High</b> in all applicable rules.</li> <li>You may choose to disable or delete rules that are not applicable to the company or reduce the Severity of these rules.</li> </ul> <p> <b>Note</b> - Before you can configure the DLP rules, you must configure the applicable objects in SmartConsole.</p>
6	Click the <b>Additional Settings &gt; Protocols</b> page. Configure these settings: <ul style="list-style-type: none"> <li>In the <b>Email</b> section, select <b>SMTP (Outgoing Emails)</b>.</li> <li>In the <b>Web</b> section, select <b>HTTP</b>. Do not configure the <b>HTTPS</b>.</li> <li>In the <b>File Transfer</b> section, do not select <b>FTP</b>.</li> </ul>
7	Click <b>Launch Menu &gt; File &gt; Update</b> (or press the <b>CTRL S</b> keys).
8	Close the SmartDashboard.
9	Install the Access Control Policy on the Security Gateway object.

Step	Instructions
10	<p>Make sure the Security Gateway enabled the SMTP Mirror Port Mode:</p> <ol style="list-style-type: none"><li>Connect to the command line on the Security Gateway.</li><li>Log in to the Expert mode.</li><li>Run this command:<pre>dlp_smtp_mirror_port status</pre></li><li>Make sure the value of the kernel parameter <code>dlp_force_smtp_kernel_inspection</code> is set to 1 (one). Run these two commands:<pre>fw ctl get int dlp_force_smtp_kernel_inspection grep dlp_force_smtp_kernel_inspection \$FWDIR/boot/modules/fwkern.conf</pre></li></ol>

**For more information:**

See the [\*R80.40 Data Loss Prevention Administration Guide\*](#).

# Configuring the Security Gateway in Monitor Mode Behind a Proxy Server

If you connect a Proxy Server between the Security Gateway 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 " <b>X Forward-For header</b> ". See the applicable documentation for your Proxy Server.
2	On the Security Gateway in Monitor Mode, enable the stripping of the X-Forward-For (XFF) field. Follow the <a href="#">sk100223: How to enable stripping of X-Forward-For (XFF) field</a> .

# Deploying a Security Gateway or a ClusterXL in Bridge Mode

## Introduction to Bridge Mode

If you cannot divide the existing network into several networks with different IP addresses, you can install a Check Point Security Gateway (or a ClusterXL) in the Bridge Mode.

A Security Gateway (or ClusterXL) in Bridge Mode is invisible to Layer 3 traffic.

When traffic arrives at one of the bridge slave interfaces, the Security Gateway (or Cluster Members) inspects it and passes it to the second bridge slave interface.

## Supported Software Blades in Bridge Mode

This table lists Software Blades, features, and their support for the Bridge Mode.

This table applies to single Security Gateway deployment, ClusterXL (with one switch) in Active/Active and Active/Standby deployment, and ClusterXL with four switches.

Software Blade	Support of a Security Gateway in Bridge Mode	Support of a ClusterXL in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Firewall	Yes	Yes	Yes
IPS	Yes	Yes	Yes
URL Filtering	Yes	Yes	Yes
DLP	Yes	Yes	No
Anti-Bot	Yes	Yes	Yes
Anti-Virus	Yes (1)	Yes (1)	Yes (1)
Application Control	Yes	Yes	Yes
HTTPS Inspection	Yes (2)	Yes (2)	No
Identity Awareness	Yes (3)	Yes (3)	No
Threat Emulation - ThreatCloud emulation	Yes	Yes	Yes in Active/Active Bridge Mode No in Active/Standby Bridge Mode

Software Blade	Support of a Security Gateway in Bridge Mode	Support of a ClusterXL in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Threat Emulation - Local emulation	Yes	Yes	No in all Bridge Modes
Threat Emulation - Remote emulation	Yes	Yes	Yes in Active/Active Bridge Mode No in Active/Standby Bridge Mode
UserCheck	Yes	Yes	No
QoS	Yes (see <a href="#">sk89581</a> )	No (see <a href="#">sk89581</a> )	No (see <a href="#">sk79700</a> )
HTTP / HTTPS proxy	Yes	Yes	No
Security Servers - SMTP, HTTP, FTP, POP3	Yes	Yes	No
Client Authentication	Yes	Yes	No
User Authentication	Yes	Yes	No
Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on)	Yes	No	No
IPsec VPN	No	No	No
Mobile Access	No	No	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 a single 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:

- Assigning an IP address to a Bridge interface in ClusterXL.
- 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.
- Clusters with more than two Cluster Members..
- Full High Availability Cluster.
- Asymmetric traffic inspection in ClusterXL in Active/Active Bridge Mode.

(Asymmetric traffic inspection is any situation, where the Client-to-Server packet is inspected by one Cluster Member, while the Server-to-Client packet is inspected by the other Cluster Member. In such scenarios, several security features do not work.)

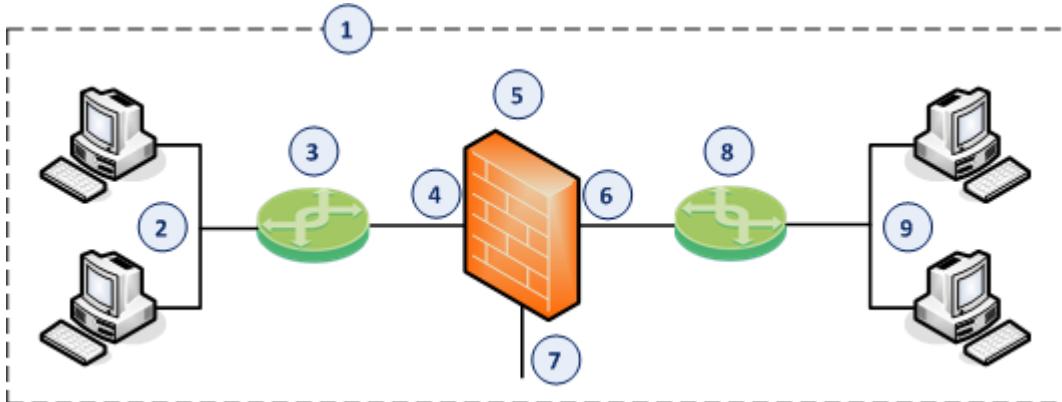
For more information, see [sk101371: Bridge Mode on Gaia OS and SecurePlatform OS](#).

# Configuring a Single Security Gateway in Bridge Mode



**Note** - This procedure applies to both Check Point Appliances and Open Servers.

## Example Topology for a single Security Gateway



Item	Description
1	Network, which an administrator needs to divide into two Layer 2 segments. The Security Gateway 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 Gateway in Bridge Mode.
4	One bridged slave interface (for example, <code>eth1</code> ) on the Security Gateway in Bridge Mode.
5	Security Gateway in Bridge Mode.
6	Another bridged slave interface (for example, <code>eth2</code> ) on the Security Gateway in Bridge Mode.
7	Dedicated Gaia Management Interface (for example, <code>eth0</code> ) on the Security Gateway.
8	Switch that connects the second network segment to the other bridged slave interface (6) on the Security Gateway in Bridge Mode.
9	Second network segment.

**Procedure:****1. Install the Security Gateway**

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38.</a>
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Management Connection</b> window, select the interface, through which you connect to Gaia operating system.</li> <li>■ In the <b>Internet Connection</b> window, do not configure IP addresses.</li> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window:               <ol style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster, type</b>.</li> </ol> </li> <li>■ In the <b>Dynamically Assigned IP</b> window, select <b>No</b>.</li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

**2. Configure the Bridge interface on the Security Gateway**

You configure the Bridge interface in either Gaia Portal, or Gaia CliSh.

**Configuring the Bridge interface in Gaia Portal**

Step	Instructions
1	In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b> .
2	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned.
3	Click <b>Add &gt; Bridge</b> . To configure an existing Bridge interface, select the Bridge interface and click <b>Edit</b> .
4	On the <b>Bridge</b> tab, enter or select a <b>Bridge Group</b> ID (unique integer between 1 and 1024).
5	Select the interfaces from the <b>Available Interfaces</b> list and then click <b>Add</b> . <b>Notes:</b> <ul style="list-style-type: none"> <li> Make sure that the slave interfaces do not have any IP addresses or aliases configured.</li> <li>Do not select the interface that you configured as Gaia Management Interface.</li> <li>A Bridge interface in Gaia can contain only two slave interfaces.</li> </ul>

Step	Instructions
6	On the <b>IPv4</b> tab, enter the IPv4 address and subnet mask. You can optionally select the <b>Obtain IPv4 Address automatically</b> option.
7	On the <b>IPv6</b> tab (optional), enter the IPv6 address and mask length. You can optionally select the <b>Obtain IPv6 Address automatically</b> option.
8	 <b>Important</b> - First, you must enable the IPv6 Support and reboot. Click <b>OK</b> .



**Note** - The name of a Bridge interface in Gaia is "*br<Bridge Group ID>*". For example, the name of a bridge interface with a Bridge Group ID of 5 is "br5".

### Configuring the Bridge interface in Gaia Clish

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to Gaia Clish.
3	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned: <pre>show interface &lt;Name of Interface&gt; ipv4-address show interface &lt;Name of Interface&gt; ipv6-address</pre>
4	Add a new bridging group: <pre>add bridging group &lt;Bridge Group ID 0 - 1024&gt;</pre>
5	Add slave interfaces to the new bridging group: <pre>add bridging group &lt;Bridge Group ID&gt; interface &lt;Name of First Slave Interface&gt; add bridging group &lt;Bridge Group ID&gt; interface &lt;Name of Second Slave Interface&gt;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Do not select the interface that you configured as Gaia Management Interface.</li> <li>■ A Bridge interface in Gaia can contain only two slave interfaces.</li> </ul>

Step	Instructions
6	<p>Assign an IP address to the bridging group.</p> <ul style="list-style-type: none"> <li>■ To assign an IPv4 address, run:</li> </ul> <pre>set interface &lt;Name of Bridge Interface&gt; ipv4- address &lt;IPv4 Address&gt; {subnet-mask &lt;Mask&gt;   mask- length &lt;Mask Length&gt;}</pre> <p>You can optionally configure the bridging group to obtain an IPv4 Address automatically.</p> <ul style="list-style-type: none"> <li>■ To assign an IPv6 address, run:</li> </ul> <pre>set interface &lt;Name of Bridge Interface&gt; ipv6- address &lt;IPv6 Address&gt; mask-length &lt;Mask Length&gt;</pre> <p>You can optionally configure the bridging group to obtain an IPv6 Address automatically.</p> <p> <b>Important</b> - First, you must enable the IPv6 Support and reboot.</p>
7	<p>Save the configuration:</p> <pre>save config</pre>



**Note** - The name of a Bridge interface in Gaia is "br<Bridge Group ID>". For example, the name of a bridge interface with a Bridge Group ID of 5 is "br5".

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

You can configure the ClusterXL 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 Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New</b> (*) &gt; <b>Gateway</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>New Gateway</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Gateway</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Creation</b> window, click <b>Wizard Mode</b> .

Step	Instructions
5	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Gateway name</b> field, enter the applicable name for this Security Gateway object.</li> <li>In the <b>Gateway platform</b> field, select the correct hardware type.</li> <li>In the <b>Gateway IP address</b> section, select <b>Static IP address</b> and configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Gateway's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> <li>Click <b>Next</b>.</li> </ol>
6	<p>On the <b>Trusted Communication</b> page:</p> <ol style="list-style-type: none"> <li>Select the applicable option: <ul style="list-style-type: none"> <li>If you selected <b>Initiate trusted communication now</b>, enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>If you selected <b>Skip and initiate trusted communication later</b>, make sure to follow Step 7.</li> </ul> </li> <li>Click <b>Next</b>.</li> </ol>
7	<p>On the <b>End</b> page:</p> <ol style="list-style-type: none"> <li>Examine the <b>Configuration Summary</b>.</li> <li>Select <b>Edit Gateway properties for further configuration</b>.</li> <li>Click <b>Finish</b>.</li> </ol> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
8	<p>If during the Wizard Mode, you selected <b>Skip and initiate trusted communication later</b>:</p> <ol style="list-style-type: none"> <li>The <b>Secure Internal Communication</b> field shows <b>Uninitialized</b>.</li> <li>Click <b>Communication</b>.</li> <li>In the <b>Platform</b> field: <ul style="list-style-type: none"> <li>Select <b>Open server / Appliance</b> for all Check Point models 3000 and higher.</li> <li>Select <b>Open server / Appliance</b> for an Open Server.</li> </ul> </li> <li>Enter the same <b>Activation Key</b> you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>. Make sure the <b>Certificate state</b> field shows <b>Established</b>.</li> <li>Click <b>OK</b>.</li> </ol>
9	<p>On the <b>General Properties</b> page:</p> <ul style="list-style-type: none"> <li>On the <b>Network Security</b> tab, enable the applicable Software Blades.</li> <li>On the <b>Threat Prevention</b> tab, enable the applicable Software Blades.</li> </ul> <p><b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726</a>".</p>



Step	Instructions
10	<p>On the <b>Network Management</b> page, configure the <b>Topology</b> of the Bridge interface.</p> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>▪ If a Bridge interface connects to the Internet, then set the <b>Topology</b> to <b>External</b>.</li> <li>▪ If you use this Bridge Security Gateway object in Access Control Policy rules with <b>Internet</b> objects, then set the <b>Topology</b> to <b>External</b>.</li> </ul>
11	Click <b>OK</b> .
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

### Configuring the Security Gateway object in Classic Mode

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

Step	Instructions
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:</p> <ol style="list-style-type: none"> <li>Near the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>In the <b>Platform</b> field: <ul style="list-style-type: none"> <li>Select <b>Open server / Appliance</b> for all Check Point models 3000 and higher.</li> <li>Select <b>Open server / Appliance</b> for an Open Server.</li> </ul> </li> <li>Enter the same <b>Activation Key</b> you entered during the Security Gateway's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>OK</b>.</li> </ol> <p>If the <b>Certificate state</b> field does not show <b>Established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Gateway.</li> <li>Make sure there is a physical connectivity between the Security Gateway and the Management Server (for example, pings can pass).</li> <li>Run:  <pre>cpconfig</pre> </li> <li>Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
8	<p>In the <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>In the <b>Hardware</b> field: <ul style="list-style-type: none"> <li>If you install the Security Gateway on a Check Point Appliance, select the correct appliances series.</li> <li>If you install the Security Gateway on an Open Server, select <b>Open server</b>.</li> </ul> </li> <li>In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
9	<p>Enable the applicable Software Blades:</p> <ul style="list-style-type: none"> <li>On the <b>Network Security</b> tab.</li> <li>On the <b>Threat Prevention</b> tab.</li> </ul> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726</a>".</p>

Step	Instructions
10	<p>On the <b>Network Management</b> page, configure the <b>Topology</b> of the Bridge interface.</p> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>▪ If a Bridge interface connects to the Internet, then set the <b>Topology</b> to <b>External</b>.</li> <li>▪ If you use this Bridge Security Gateway object in Access Control Policy rules with <b>Internet</b> objects, then set the <b>Topology</b> to <b>External</b>.</li> </ul>
11	Click <b>OK</b> .
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

#### 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 Gateway.
2	From the left navigation panel, click <b>Security Policies</b> .
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> <li>a. At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>b. On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>c. In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>d. Click <b>Close</b>.</li> <li>e. On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>
4	<p>Create the applicable rules in the Access Control and Threat Prevention policies.</p>  <p><b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726</a>.</p>
5	Install the Access Control Policy on the Security Gateway object.
5	Install the Threat Prevention Policy on the Security Gateway object.

For more information, see the:

- [R80.40 Gaia Administration Guide](#).
- [R80.40 Security Management Administration Guide](#).
- Applicable *Administration Guides* on the [R80.40 Home Page](#).

# Configuring a ClusterXL in Bridge Mode

You can configure ClusterXL in Bridge Mode in different cluster deployments:

Bridge Mode	Number of Supported Switches
Active/Standby Bridge Mode	Two only
Active/Active Bridge Mode	Two, or Four

For instructions, see:

- [\*"Configuring ClusterXL in Bridge Mode - Active / Standby with Two Switches" on page 738\*](#)
- [\*"Configuring ClusterXL in Bridge Mode - Active / Active with Two or Four Switches" on page 752\*](#)

# Configuring ClusterXL in Bridge Mode - Active / Standby with Two Switches

## Notes:



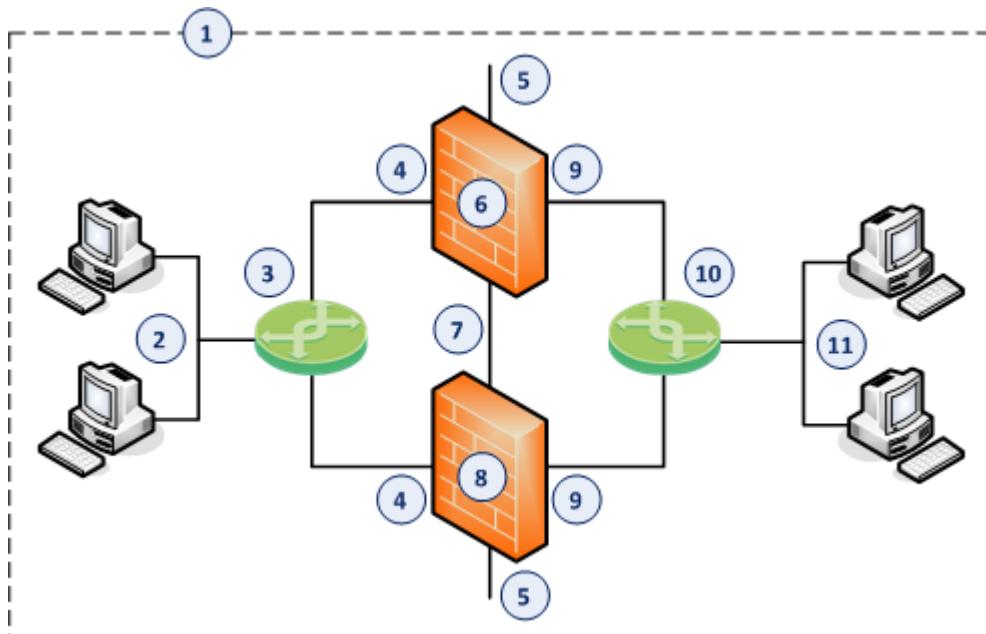
- This procedure applies to both Check Point Appliances and Open Servers.
- ClusterXL deployed in Active/Standby Bridge Mode, supports only two switches.

The Active/Standby Bridge Mode is the preferred mode in topologies that support it.

In the Active/Standby Bridge Mode, Cluster Members work in High Availability mode.

For more information, see the [R80.40 ClusterXL Administration Guide](#).

## Example Topology with Two Switches



Item	Instructions
1	Network, which an administrator needs to divide into two Layer 2 segments. The ClusterXL 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 ClusterXL in Bridge Mode.
4	One bridged slave interface (for example, <code>eth1</code> ) on the Cluster Members in Bridge Mode.
5	Dedicated Gaia Management Interface (for example, <code>eth0</code> ) on the Cluster Members.
6	First Cluster Member in Bridge Mode (for example, in the <code>Active</code> cluster state).

Item	Instructions
7	Network that connects dedicated synchronization interfaces (for example, <code>eth3</code> ) on the ClusterXL in Bridge Mode.
8	Second Cluster Member in Bridge Mode (for example, in the <code>Standby</code> cluster state).
9	Another bridged slave interface (for example, <code>eth2</code> ) on the Cluster Members in Bridge Mode.
10	Switch that connects the second network segment to the other bridged slave interface (9) on the ClusterXL in Bridge Mode.
11	Second network segment.

#### Procedure:



**Best Practice** - If you configure Bridge Mode Active / Standby, then disable STP, RSTP, and MSTP on the adjacent switches. See the applicable documentation for your switches.

#### 1. Install the two Cluster Members

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, select these two options: <ul style="list-style-type: none"> <li>• <b>Unit is a part of a cluster</b></li> <li>• <b>ClusterXL</b></li> </ul> </li> </ul> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

#### 2. Configure the ClusterXL object in High Availability mode in SmartConsole

You can configure the ClusterXL object in either Wizard Mode, or Classic Mode.

## Configuring the ClusterXL object in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this ClusterXL.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new Cluster object in one of these ways: <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★)</b> &gt; <b>Cluster</b> &gt; <b>Cluster</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Cluster</b> &gt; <b>New Cluster</b>.</li> <li>■ In the top right corner, click <b>Objects Pane</b> &gt; <b>New</b> &gt; <b>More</b> &gt; <b>Network Object</b> &gt; <b>Gateways and Servers</b> &gt; <b>Cluster</b> &gt; <b>Cluster</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Cluster Creation</b> window, click <b>Wizard Mode</b> .
5	On the <b>Cluster General Properties</b> page: <ol style="list-style-type: none"> <li>a. In the <b>Cluster Name</b> field, enter the applicable name for this ClusterXL object.</li> <li>b. Configure the main Virtual IP address(es) for this ClusterXL object. In the <b>Cluster IPv4 Address</b> section, enter the main Virtual IPv4 address for this ClusterXL object. In the <b>Cluster IPv6 Address</b> section, enter the main Virtual IPv6 address for this ClusterXL object.</li> <li>c. In the <b>Choose the Cluster's Solution</b> field, select <b>Check Point ClusterXL</b> and <b>High Availability</b>.</li> <li>d. Click <b>Next</b>.</li> </ol>

Step	Instructions
6	<p>On the <b>Cluster members' properties</b> page, add the objects for the Cluster Members.</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p><b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. In the <b>Activation Key</b> and <b>Confirm Activation Key</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>e. Click <b>Initialize</b>.</li> <li>f. Click <b>OK</b>.</li> <li>g. Repeat Steps a-f to add the second Cluster Member, and so on.</li> </ol> <p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the Cluster Member.</li> <li>b. Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).</li> <li>c. Run: <code>cpconfig</code></li> <li>d. Enter the number of this option: <code>Secure Internal Communication</code></li> <li>e. Follow the instructions on the screen to change the Activation Key.</li> <li>f. In SmartConsole, click <b>Reset</b>.</li> <li>g. Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>h. In SmartConsole, click <b>Initialize</b>.</li> </ol>

Step	Instructions
7	<p>On the <b>Cluster Topology</b> page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>IPv4 Network Address</b> at the top of the page.</li> <li>b. Select the applicable role: <ul style="list-style-type: none"> <li>■ For <i>cluster traffic interfaces</i>, select <b>Representing a cluster interface</b> and configure the Cluster Virtual IPv4 address and its Net Mask.</li> <li> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</li> <li>■ For <i>cluster synchronization interfaces</i>, select <b>Cluster Synchronization</b> and select <b>Primary</b> only. Check Point cluster supports only one synchronization network.</li> <li>■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private use of each member (don't monitor members interfaces)</b>.</li> </ul> </li> <li>c. Click <b>Next</b></li> </ol>
8	<p>On the <b>Cluster Definition Wizard Complete</b> page:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>Configuration Summary</b>.</li> <li>b. Select <b>Edit Cluster's Properties</b>.</li> <li>c. Click <b>Finish</b></li> </ol> <p>The <b>Gateway Cluster Properties</b> window opens.</p>
9	<p>On the <b>General Properties</b> page &gt; <b>Machine</b> section:</p> <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, make sure you see the configured applicable name for this ClusterXL object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard.</li> </ol> <p>Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p>
10	<p>On the <b>General Properties</b> page &gt; <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
11	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL</b> Software Blade is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ol> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726</a>".</p>

Step	Instructions
12	<p>On the <b>Cluster Members</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>Click <b>Communication</b>.</li> <li>In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>Close</b>.</li> <li>Click <b>OK</b>.</li> <li>Repeat Steps <b>a-h</b> to add the second Cluster Member, and so on.</li> </ol> <p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Cluster Member.</li> <li>Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).</li> <li>Run: <code>cpconfig</code></li> <li>Enter the number of this option: <code>Secure Internal Communication</code></li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>

Step	Instructions
13	<p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"><li>In the <b>Select the cluster mode and configuration</b> section, select <b>High Availability</b> and <b>ClusterXL</b>.</li><li>In the <b>Tracking</b> section, select the applicable option.</li><li>In the <b>Advanced Settings</b> section:<ol style="list-style-type: none"><li><b>Optional:</b> Select <b>Use State Synchronization</b>.  <b>Best Practice</b> - We recommend to select this option. For more information, click the (?) button in the top right corner.</li><li><b>Optional:</b> Select <b>Use Virtual MAC</b>. For more information, see <a href="#">sk50840</a>.</li><li>Select the Cluster Member recovery method. For more information, click the (?) button in the top right corner.</li></ol></li></ol>

Step	Instructions
14	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li>From the left tree, click the <b>General</b> page.</li> <li>In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type: <ul style="list-style-type: none"> <li>■ For <i>cluster traffic interfaces</i>, select <b>Cluster</b>. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li>■ For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li>• Check Point cluster supports only one synchronization network.</li> <li>• For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li>■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li>In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <p>e. In the <b>Topology</b> section:</p> <ul style="list-style-type: none"> <li>■ Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li>■ Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure the Bridge interface and Bridge slave interfaces are <b>not</b> in the Topology.</li> <li>■ You cannot define the <b>Topology</b> of the Bridge interface. It is <b>External</b> by default.</li> </ul>
15	Click <b>OK</b> .
16	Publish the SmartConsole session.

### Configuring the ClusterXL object in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this ClusterXL.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★) &gt; Cluster &gt; Cluster</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; New Cluster</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; Cluster</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>. The <b>Gateway Cluster Properties</b> window opens.</p>
5	<p>On the <b>General Properties</b> page &gt; <b>Machine</b> section:</p> <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, make sure you see the configured applicable name for this ClusterXL object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol>
6	<p>On the <b>General Properties</b> page &gt; <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
7	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL</b> Software Blade is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ol> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726</a>".</p>

Step	Instructions
8	<p>On the <b>Cluster Members</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p><b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>Click <b>Communication</b>.</li> <li>In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>Close</b>.</li> <li>Click <b>OK</b>.</li> <li>Repeat Steps <b>a-h</b> to add the second Cluster Member, and so on.</li> </ol>

If the **Trust State** field does not show **Trust established**, perform these steps:

- Connect to the command line on the Cluster Member.
- Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).
- Run:  

```
cpconfig
```
- Enter the number of this option:  

```
Secure Internal Communication
```
- Follow the instructions on the screen to change the Activation Key.
- In SmartConsole, click **Reset**.
- Enter the same Activation Key you entered in the **cpconfig** menu.
- In SmartConsole, click **Initialize**.

Step	Instructions
9	<p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"><li>In the <b>Select the cluster mode and configuration</b> section, select <b>High Availability</b> and <b>ClusterXL</b>.</li><li>In the <b>Tracking</b> section, select the applicable option.</li><li>In the <b>Advanced Settings</b> section:<ol style="list-style-type: none"><li><b>Optional:</b> Select <b>Use State Synchronization</b>.  <b>Best Practice</b> - We recommend to select this option. For more information, click the (?) button in the top right corner.</li><li><b>Optional:</b> Select <b>Use Virtual MAC</b>. For more information, see <a href="#">sk50840</a>.</li><li>Select the Cluster Member recovery method. For more information, click the (?) button in the top right corner.</li></ol></li></ol>

Step	Instructions
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li>From the left tree, click the <b>General</b> page.</li> <li>In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type: <ul style="list-style-type: none"> <li>■ For <i>cluster traffic interfaces</i>, select <b>Cluster</b>. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li>■ For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li>• Check Point cluster supports only one synchronization network.</li> <li>• For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li>■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li>In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <ol style="list-style-type: none"> <li>In the <b>Topology</b> section: <ul style="list-style-type: none"> <li>■ Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li>■ Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> </li> </ol> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure the Bridge interface and Bridge slave interfaces are <b>not</b> in the Topology.</li> <li>■ You cannot define the <b>Topology</b> of the Bridge interface. It is <b>External</b> by default.</li> </ul>
11	Click <b>OK</b> .
12	Publish the SmartConsole session.

### 3. Configure the applicable Security Policies for the ClusterXL in SmartConsole

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

Step	Instructions
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> <li>At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>Click <b>Close</b>.</li> <li>On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>
4	<p>Create the applicable rules in the Access Control and Threat Prevention policies.</p> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">Deploying a Security Gateway or a ClusterXL in Bridge Mode</a>" on page 726.</p>
5	Install the Access Control Policy on the ClusterXL object.
6	Install the Threat Prevention Policy on the ClusterXL object.

#### 4. Examine the cluster configuration

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">show cluster state</div> <li>■ In the Expert mode, run:</li> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">cphaprof state</div> </ul> <p><b>Example output:</b></p> <div style="border: 1px solid black; padding: 10px; background-color: #f9f9f9;"> <pre>Member1&gt; show cluster state  Cluster Mode:  High Availability (Active Up) with IGMP Membership  ID      Unique Address  Assigned Load   State      Name 1 (local)  11.22.33.245  100%          ACTIVE     Member1 2          11.22.33.246  0%            STANDBY    Member2</pre> </div>
3	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> <li>■ In Gaia Clish, run:</li> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">show cluster members interfaces all</div> <li>■ In the Expansion Line Card, run:</li> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">cphaprof -a if</div> </ul>

#### 5. Enable the Active/Standby Bridge Mode on both Cluster Members

Item	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Run: <pre>cpcconfig</pre>
3	Select <b>Enable Check Point ClusterXL for Bridge Active/Standby</b> .
4	Enter <b>y</b> to confirm.
5	Reboot <i>each</i> Cluster Member.
6	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this ClusterXL.
7	Install the Access Control Policy on this cluster object.

## 6. Examine the cluster configuration

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: <pre>show cluster state</pre></li> <li>■ In the Expert mode, run: <pre>cphaprof state</pre></li> </ul> <p>Example output:</p> <pre>Member1&gt; show cluster state  Cluster Mode: High Availability (Active Up, <b>Bridge Mode</b>) with IGMP Membership  ID      Unique Address  Assigned Load    State      Name 1 (local)  11.22.33.245   100%          ACTIVE     Member1 2           11.22.33.246    0%            STANDBY   Member2</pre>
3	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: <pre>show cluster members interfaces all</pre></li> <li>■ In the Expansion Line Card, run: <pre>cphaprof -a if</pre></li> </ul>

# Configuring ClusterXL in Bridge Mode - Active / Active with Two or Four Switches

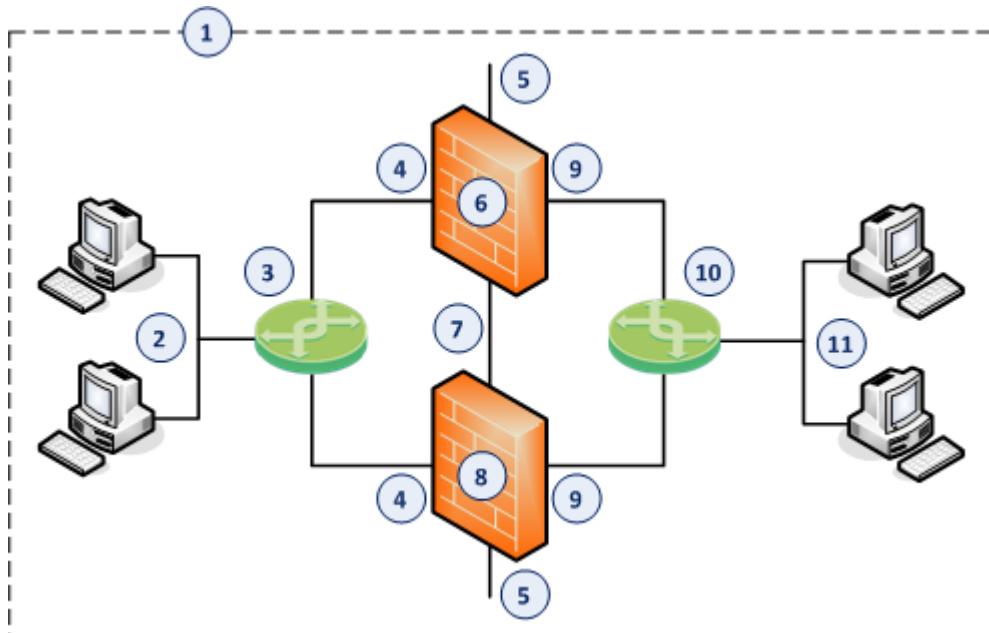
When you define a Bridge interface on a Cluster Member, the Active/Active Bridge Mode is enabled by default.

## Notes:



- This procedure applies to both Check Point Appliances and Open Servers.
- This procedure describes ClusterXL in Active/Active Bridge Mode deployed with two or four switches.

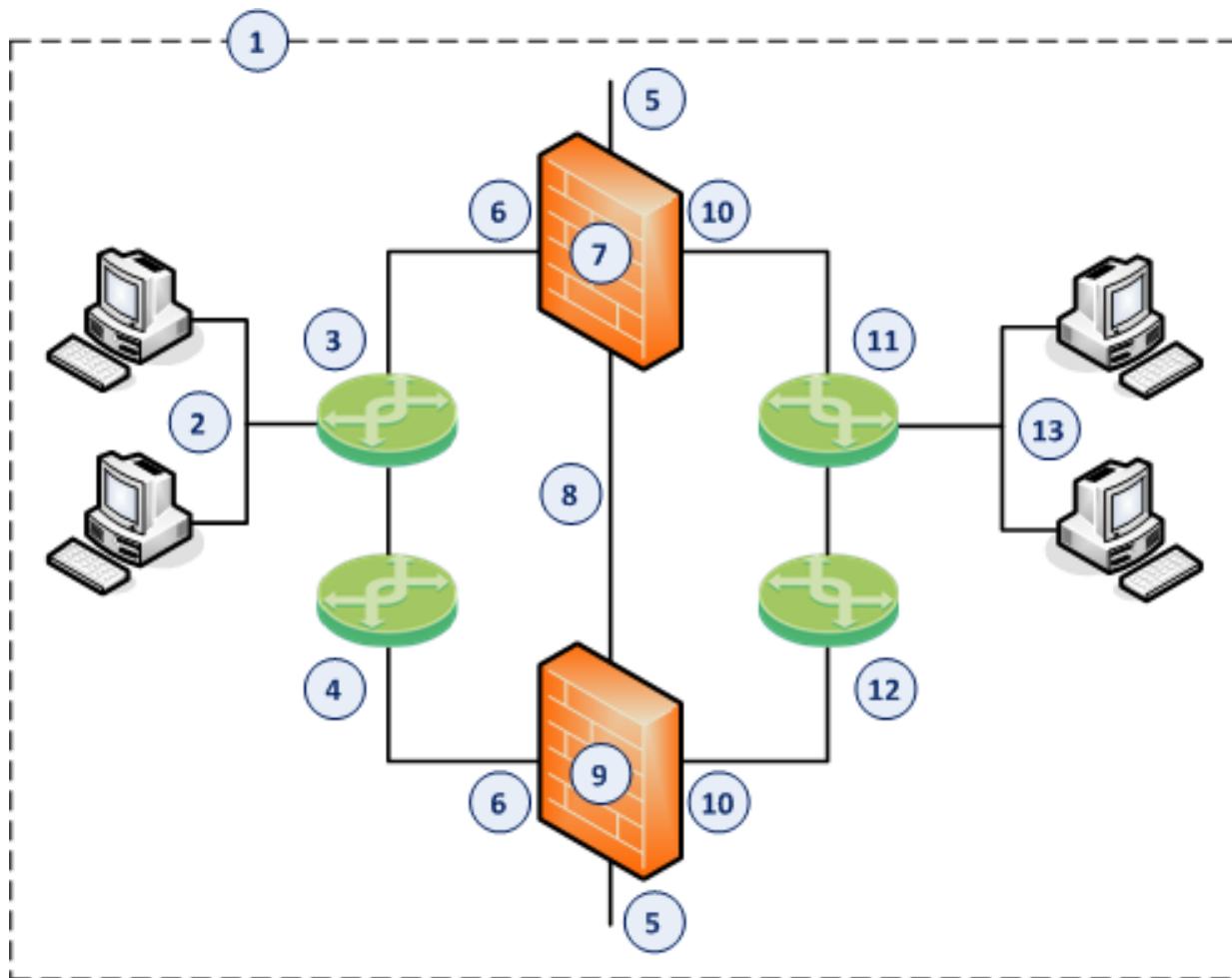
## Example Topology with Two Switches



Item	Instructions
1	Network, which an administrator needs to divide into two Layer 2 segments. The ClusterXL 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 ClusterXL in Bridge Mode.
4	One bridged slave interface (for example, eth1) on the Cluster Members in Bridge Mode.
5	Dedicated Gaia Management Interface (for example, eth0) on the Cluster Members.
6	First Cluster Member in Bridge Mode (in the <code>Active</code> cluster state).
7	Network that connects dedicated synchronization interfaces (for example, eth3) on the ClusterXL in Bridge Mode.
8	Second Cluster Member in Bridge Mode (in the <code>Active</code> cluster state).

Item	Instructions
9	Another bridged slave interface (for example, eth2) on the Cluster Members in Bridge Mode.
10	Switch that connects the second network segment to the other bridged slave interface (9) on the ClusterXL in Bridge Mode.
11	Second network segment.

### Example Topology with Four Switches



Item	Instructions
1	Network, which an administrator needs to divide into two Layer 2 segments. The ClusterXL in Bridge Mode connects between these segments.
2	First network segment.
3	Switch that connects the first network segment to one bridged slave interface (6) on the ClusterXL in Bridge Mode.
4	Switch that connects between one switch (that directly connects to the first network segment) and one bridged slave interface (6) on the ClusterXL in Bridge Mode.

Item	Instructions
5	Dedicated Gaia Management Interface (for example, eth0) on the Cluster Members.
6	One bridged slave interface (for example, eth1) on the Cluster Members in Bridge Mode.
7	First Cluster Member in Bridge Mode (in the <code>Active</code> cluster state).
8	Network that connects dedicated synchronization interfaces (for example, eth3) on the ClusterXL in Bridge Mode.
9	Second Cluster Member in Bridge Mode (in the <code>Active</code> cluster state).
10	Another bridged slave interface (for example, eth2) on the Cluster Members in Bridge Mode.
11	Switch that connects the second network segment to the other bridged slave interface (10) on the ClusterXL in Bridge Mode.
12	Switch that connects between one switch (that directly connects to the second network segment) and the other bridged slave interface (10) on the ClusterXL in Bridge Mode.
13	Second network segment.

#### Procedure:

##### 1. Install the two Cluster Members

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> <li>■ <a href="#">"Installing the Gaia Operating System on Check Point Appliances" on page 31</a></li> <li>■ <a href="#">"Installing the Gaia Operating System on Open Servers" on page 33</a></li> </ul>
2	Follow <a href="#">"Configuring Gaia for the First Time" on page 38</a> .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> <li>■ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>■ In the <b>Products</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, select these two options: <ul style="list-style-type: none"> <li>• <b>Unit is a part of a cluster</b></li> <li>• <b>ClusterXL</b></li> </ul> </li> </ul> </li> <li>■ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

##### 2. Configure the Bridge interface on both Cluster Members

You configure the Bridge interface in either Gaia Portal, or Gaia Clish.

## Configuring the Bridge interface in Gaia Portal

Step	Instructions
1	In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b> .
2	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned.
3	Click <b>Add &gt; Bridge</b> . To configure an existing Bridge interface, select the Bridge interface and click <b>Edit</b> .
4	On the <b>Bridge</b> tab, enter or select a <b>Bridge Group ID</b> (unique integer between 1 and 1024).
5	Select the interfaces from the <b>Available Interfaces</b> list and then click <b>Add</b> . <b>Notes:</b>  <ul style="list-style-type: none"> <li>■ Make sure that the slave interfaces do not have any IP addresses or aliases configured.</li> <li>■ Do <b>not</b> select the interface that you configured as Gaia Management Interface.</li> <li>■ A Bridge interface in Gaia can contain only two slave interfaces.</li> </ul>
6	On the <b>IPv4</b> tab, enter the IPv4 address and subnet mask. You can optionally select the <b>Obtain IPv4 Address automatically</b> option.
7	On the <b>IPv6</b> tab (optional), enter the IPv6 address and mask length. You can optionally select the <b>Obtain IPv6 Address automatically</b> option.   <b>Important</b> - First, you must enable the IPv6 Support and reboot.
8	Click <b>OK</b> .



**Note** - The name of a Bridge interface in Gaia is "*br<Bridge Group ID>*". For example, the name of a bridge interface with a Bridge Group ID of 5 is "*br5*".

## Configuring the Bridge interface in Gaia Clish

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	Log in to Gaia Clish.
3	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned: <div style="border: 1px solid black; padding: 5px; margin-left: 20px;"> <pre>show interface &lt;Name of Interface&gt; ipv4-address show interface &lt;Name of Interface&gt; ipv6-address</pre> </div>

Step	Instructions
4	<p>Add a new bridging group:</p> <pre>add bridging group &lt;Bridge Group ID 0 - 1024&gt;</pre>
5	<p>Add slave interfaces to the new bridging group:</p> <pre>add bridging group &lt;Bridge Group ID&gt; interface &lt;Name of First Slave Interface&gt; add bridging group &lt;Bridge Group ID&gt; interface &lt;Name of Second Slave Interface&gt;</pre> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ A Bridge interface in Gaia can contain only two slave interfaces.</li> <li>■ Do not select the interface that you configured as Gaia Management Interface.</li> </ul>
6	Do not assign an IP address to the bridging group.
7	<p>Save the configuration:</p> <pre>save config</pre>



**Note** - The name of a Bridge interface in Gaia is "br<Bridge Group ID>". For example, the name of a bridge interface with a Bridge Group ID of 5 is "br5".

### 3. Configure the ClusterXL object in SmartConsole

You can configure the ClusterXL object in either Wizard Mode, or Classic Mode.

#### Configuring the ClusterXL object in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this ClusterXL.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new Cluster object in one of these ways: <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★) &gt; Cluster &gt; Cluster</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; New Cluster</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; Cluster</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Cluster Creation</b> window, click <b>Wizard Mode</b> .

Step	Instructions
5	<p>On the <b>Cluster General Properties</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Cluster Name</b> field, enter the applicable name for this ClusterXL object.</li> <li>Configure the main Virtual IP address(es) for this ClusterXL object. <ul style="list-style-type: none"> <li>In the <b>Cluster IPv4 Address</b> section, enter the main Virtual IPv4 address for this ClusterXL object.</li> <li>In the <b>Cluster IPv6 Address</b> section, enter the main Virtual IPv6 address for this ClusterXL object.</li> </ul> </li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>In the <b>Choose the Cluster's Solution</b> field, select <b>Check Point ClusterXL</b> and select the cluster mode - either <b>High Availability</b>, or <b>Load Sharing</b>.</li> <li>Click <b>Next</b>.</li> </ol>
6	<p>On the <b>Cluster members' properties</b> page, add the objects for the Cluster Members.</p> <ol style="list-style-type: none"> <li>Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>In the <b>Activation Key</b> and <b>Confirm Activation Key</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>OK</b>.</li> <li>Repeat Steps <b>a-f</b> to add the second Cluster Member, and so on.</li> </ol>

Step	Instructions
	<p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the Cluster Member.</li> <li>b. Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).</li> <li>c. Run:  <pre>cpconfig</pre> </li> <li>d. Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>e. Follow the instructions on the screen to change the Activation Key.</li> <li>f. In SmartConsole, click <b>Reset</b>.</li> <li>g. Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>h. In SmartConsole, click <b>Initialize</b>.</li> </ol>
7	<p>On the <b>Cluster Topology</b> page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>IPv4 Network Address</b> at the top of the page.</li> <li>b. Select the applicable role: <ul style="list-style-type: none"> <li>■ For <i>cluster traffic interfaces</i>, select <b>Representing a cluster interface</b> and configure the Cluster Virtual IPv4 address and its Net Mask.    <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</li> <li>■ For <i>cluster synchronization interfaces</i>, select <b>Cluster Synchronization</b> and select <b>Primary</b> only. Check Point cluster supports only one synchronization network.</li> <li>■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private use of each member (don't monitor members interfaces)</b>.</li> </ul> </li> <li>c. Click <b>Next</b></li> </ol>
8	<p>On the <b>Cluster Definition Wizard Complete</b> page:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>Configuration Summary</b>.</li> <li>b. Select <b>Edit Cluster's Properties</b>.</li> <li>c. Click <b>Finish</b></li> </ol> <p>The <b>Gateway Cluster Properties</b> window opens.</p>
9	<p>On the <b>General Properties</b> page &gt; <b>Machine</b> section:</p> <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, make sure you see the configured applicable name for this ClusterXL object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard.  <p>Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p> </li> </ol>

Step	Instructions
10	<p>On the <b>General Properties</b> page &gt; <b>Platform</b> section, select the correct options:</p> <ul style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ul>
11	<p>On the <b>General Properties</b> page:</p> <ul style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL</b> Software Blade is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ul> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726</a>".</p>
12	<p>On the <b>Cluster Members</b> page:</p> <ul style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ul> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ul style="list-style-type: none"> <li>d. Click <b>Communication</b>.</li> <li>e. In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>f. Click <b>Initialize</b>.</li> <li>g. Click <b>Close</b>.</li> <li>h. Click <b>OK</b>.</li> <li>i. Repeat Steps <b>a-h</b> to add the second Cluster Member, and so on.</li> </ul>

Step	Instructions
	<p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Cluster Member.</li> <li>Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).</li> <li>Run:  <pre>cpconfig</pre> </li> <li>Enter the number of this option:  <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
13	<p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Select the cluster mode and configuration</b> section, select the applicable mode: <ul style="list-style-type: none"> <li>■ <b>High Availability</b> and <b>ClusterXL</b></li> <li>■ <b>Load Sharing</b> and <b>Multicast</b> or <b>Unicast</b></li> <li>■ <b>Active-Active</b> (see the <a href="#">R80.40 ClusterXL Administration Guide</a>)</li> </ul> </li> <li>In the <b>Tracking</b> section, select the applicable option.</li> <li>In the <b>Advanced Settings</b> section:</li> </ol>

Step	Instructions
	<ul style="list-style-type: none"> <li>■ If you selected the <b>High Availability</b> mode, then:           <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use State Synchronization</b>. This configures the Cluster Members to synchronize the information about the connections they inspect.</li> </ul> </li> </ul> <p> <b>Best Practice</b> - Enable this setting to prevent connection drops after a cluster failover.</p> <ul style="list-style-type: none"> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> <p> <b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>• The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>• The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual MAC</b> address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the Cluster Member recovery method - which Cluster Member to select as <b>Active</b> during a fallback (return to normal operation after a cluster failover):       <ul style="list-style-type: none"> <li>• <b>Maintain current active Cluster Member</b> <ul style="list-style-type: none"> <li>i. The Cluster Member that is currently in the <b>Active</b> state, remains in this state.</li> <li>ii. Other Cluster Members that return to normal operation, remain the <b>Standby</b> state.</li> </ul> </li> <li>• <b>Switch to higher priority Cluster Member</b> <ul style="list-style-type: none"> <li>i. The Cluster Member that has the highest priority (appears at the top of the list on the <b>Cluster Members</b> page of the cluster object) becomes the new <b>Active</b>.</li> <li>ii. The state of the previously <b>Active</b> Cluster Member changes to <b>Standby</b>.</li> <li>iii. Other Cluster Members that return to normal operation remain the <b>Standby</b> state.</li> </ul> </li> </ul> </li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>■ If you selected the <b>Load Sharing &gt; Multicast</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>• The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>• The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. Select the connection sharing method between the Cluster Members:             <ul style="list-style-type: none"> <li>• <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members. This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> <li>• <b>IPs, Ports</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address and the same Source and Destination ports, regardless of the IPsec SPI numbers. Use this method only if there are problems when distributing IPsec packets between Cluster Members.</li> <li>• <b>IPs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, regardless of the Source and Destination ports and IPsec SPI numbers. This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</li> </ul> </li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>■ If you selected the <b>Load Sharing &gt; Unicast</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>• The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>• The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual MAC</b> address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the connection sharing method between the Cluster Members:             <ul style="list-style-type: none"> <li>• <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members. This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> <li>• <b>IPs, Ports</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address and the same Source and Destination ports, regardless of the IPsec SPI numbers. Use this method only if there are problems when distributing IPsec packets between Cluster Members.</li> <li>• <b>IPs</b></li> </ul> </li> </ul>

Step	Instructions
14	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li>From the left tree, click the <b>General</b> page.</li> <li>In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type: <ul style="list-style-type: none"> <li>■ For <i>cluster traffic interfaces</i>, select <b>Cluster</b>. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li>■ For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li>• Check Point cluster supports only one synchronization network.</li> <li>• For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li>■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li>In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <p>e. In the <b>Topology</b> section:</p> <ul style="list-style-type: none"> <li>■ Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li>■ Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure the Bridge interface and Bridge slave interfaces are <b>not</b> in the Topology.</li> <li>■ You cannot define the <b>Topology</b> of the Bridge interface. It is <b>External</b> by default.</li> </ul>
15	Click <b>OK</b> .
16	Publish the SmartConsole session.

### Configuring the ClusterXL object in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this ClusterXL.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .

Step	Instructions
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (★) &gt; Cluster &gt; Cluster</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; New Cluster</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Cluster &gt; Cluster</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>. The <b>Gateway Cluster Properties</b> window opens.</p>
5	<p>On the <b>General Properties</b> page &gt; <b>Machine</b> section:</p> <ol style="list-style-type: none"> <li>a. In the <b>Name</b> field, make sure you see the configured applicable name for this ClusterXL object.</li> <li>b. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol>
6	<p>On the <b>General Properties</b> page &gt; <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>a. In the <b>Hardware</b> field: If you install the Cluster Members on Check Point Appliances, select the correct appliances series. If you install the Cluster Members on Open Servers, select <b>Open server</b>.</li> <li>b. In the <b>Version</b> field, select <b>R80.40</b>.</li> <li>c. In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
7	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. On the <b>Network Security</b> tab, make sure the <b>ClusterXL</b> Software Blade is selected.</li> <li>b. Enable the additional applicable Software Blades on the <b>Network Security</b> tab and on the <b>Threat Prevention</b> tab.</li> </ol> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">"Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 726</a>".</p>

Step	Instructions
8	<p>On the <b>Cluster Members</b> page:</p> <ol style="list-style-type: none"> <li>a. Click <b>Add &gt; New Cluster Member</b>. The <b>Cluster Member Properties</b> window opens.</li> <li>b. In the <b>Name</b> field, enter the applicable name for this Cluster Member object.</li> <li>c. Configure the main physical IP address(es) for this Cluster Member object. In the <b>IPv4 Address</b> and <b>IPv6 Address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> </ol> <p> <b>Note</b> - You can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members.</p> <ol style="list-style-type: none"> <li>d. Click <b>Communication</b>.</li> <li>e. In the <b>One-time password</b> and <b>Confirm one-time password</b> fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.</li> <li>f. Click <b>Initialize</b>.</li> <li>g. Click <b>Close</b>.</li> <li>h. Click <b>OK</b>.</li> <li>i. Repeat Steps a-h to add the second Cluster Member, and so on.</li> </ol>
9	<p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the Cluster Member.</li> <li>b. Make sure there is a physical connectivity between the Cluster Member and the Management Server (for example, pings can pass).</li> <li>c. Run: <code>cpconfig</code></li> <li>d. Enter the number of this option: <code>Secure Internal Communication</code></li> <li>e. Follow the instructions on the screen to change the Activation Key.</li> <li>f. In SmartConsole, click <b>Reset</b>.</li> <li>g. Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>h. In SmartConsole, click <b>Initialize</b>.</li> </ol> <p>On the <b>ClusterXL and VRRP</b> page:</p> <ol style="list-style-type: none"> <li>a. In the <b>Select the cluster mode and configuration</b> section, select the applicable mode: <ul style="list-style-type: none"> <li>■ <b>High Availability</b> and <b>ClusterXL</b></li> <li>■ <b>Load Sharing</b> and <b>Multicast or Unicast</b></li> <li>■ <b>Active-Active</b> (see the <a href="#">R80.40 ClusterXL Administration Guide</a>)</li> </ul> </li> <li>b. In the <b>Tracking</b> section, select the applicable option.</li> <li>c. In the <b>Advanced Settings</b> section:</li> </ol>

Step	Instructions
	<ul style="list-style-type: none"> <li>■ If you selected the <b>High Availability</b> mode, then:           <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use State Synchronization</b>. This configures the Cluster Members to synchronize the information about the connections they inspect.</li> </ul> </li> </ul> <p> <b>Best Practice</b> - Enable this setting to prevent connection drops after a cluster failover.</p> <ul style="list-style-type: none"> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> <p> <b>Notes:</b></p> <ul style="list-style-type: none"> <li>• This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>• The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>• The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual MAC</b> address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the Cluster Member recovery method - which Cluster Member to select as <b>Active</b> during a fallback (return to normal operation after a cluster failover):       <ul style="list-style-type: none"> <li>• <b>Maintain current active Cluster Member</b> <ul style="list-style-type: none"> <li>i. The Cluster Member that is currently in the <b>Active</b> state, remains in this state.</li> <li>ii. Other Cluster Members that return to normal operation, remain the <b>Standby</b> state.</li> </ul> </li> <li>• <b>Switch to higher priority Cluster Member</b> <ul style="list-style-type: none"> <li>i. The Cluster Member that has the highest priority (appears at the top of the list on the <b>Cluster Members</b> page of the cluster object) becomes the new <b>Active</b>.</li> <li>ii. The state of the previously <b>Active</b> Cluster Member changes to <b>Standby</b>.</li> <li>iii. Other Cluster Members that return to normal operation remain the <b>Standby</b> state.</li> </ul> </li> </ul> </li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>■ If you selected the <b>Load Sharing &gt; Multicast</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>• The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>• The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. Select the connection sharing method between the Cluster Members:             <ul style="list-style-type: none"> <li>• <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members. This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> <li>• <b>IPs, Ports</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address and the same Source and Destination ports, regardless of the IPsec SPI numbers. Use this method only if there are problems when distributing IPsec packets between Cluster Members.</li> <li>• <b>IPs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, regardless of the Source and Destination ports and IPsec SPI numbers. This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</li> </ul> </li> </ul>

Step	Instructions
	<ul style="list-style-type: none"> <li>■ If you selected the <b>Load Sharing &gt; Unicast</b> mode, then:             <ul style="list-style-type: none"> <li>i. <b>Optional:</b> Select <b>Use Sticky Decision Function</b>. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner.</li> <li>ii. <b>Optional:</b> Select <b>Start synchronizing [ ] seconds after connection initiation</b> and enter the applicable value. This option is available only for clusters R80.20 and higher. To prevent the synchronization of short-lived connections (which decreases the cluster performance), you can configure the Cluster Members to start the synchronization of <b>all</b> connections a number of seconds after they start. <b>Range:</b> 2 - 60 seconds <b>Default:</b> 3 seconds</li> </ul> </li> </ul> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• This setting in the cluster object applies to all connections that pass through the cluster. You can override this global cluster synchronization delay in the properties of applicable services - see the <a href="#">R80.40 ClusterXL Administration Guide</a>.</li> <li>• The greater this value, the fewer short-lived connections the Cluster Members have to synchronize.</li> <li>• The connections that the Cluster Members did not synchronize, do not survive a cluster failover.</li> </ul> <p> <b>Best Practice</b> - Enable and configure this setting to increase the cluster performance.</p> <ul style="list-style-type: none"> <li>iii. <b>Optional:</b> Select <b>Use Virtual MAC</b>. This configures all Cluster Members to associate the same <b>virtual MAC</b> address with the Virtual IP address on the applicable interfaces (each Virtual IP address has its unique Virtual MAC address). For more information, see <a href="#">sk50840</a>.</li> <li>iv. Select the connection sharing method between the Cluster Members:             <ul style="list-style-type: none"> <li>• <b>IPs, Ports, SPIs</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address, the same Source and Destination ports, and the same IPsec SPI numbers. This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members. This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions We recommend this method.</li> <li>• <b>IPs, Ports</b> Configures each Cluster Member to inspect all connections with the same Source and Destination IP address and the same Source and Destination ports, regardless of the IPsec SPI numbers. Use this method only if there are problems when distributing IPsec packets between Cluster Members.</li> <li>• <b>IPs</b></li> </ul> </li> </ul>

Step	Instructions
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Select each interface and click <b>Edit</b>. The <b>Network: &lt;Name of Interface&gt;</b> window opens.</li> <li>From the left tree, click the <b>General</b> page.</li> <li>In the <b>General</b> section, in the <b>Network Type</b> field, select the applicable type: <ul style="list-style-type: none"> <li>■ For <i>cluster traffic interfaces</i>, select <b>Cluster</b>. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.</li> <li>■ For <i>cluster synchronization interfaces</i>, select <b>Sync</b> or <b>Cluster+Sync</b>.</li> </ul> </li> </ol> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>• We do not recommend the configuration <b>Cluster+Sync</b>.</li> <li>• Check Point cluster supports only one synchronization network.</li> <li>• For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</li> <li>■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select <b>Private</b>.</li> </ul> <ol style="list-style-type: none"> <li>In the <b>Member IPs</b> section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</li> </ol> <p><b>Note</b> - For <i>cluster traffic interfaces</i>, you can configure the Cluster Virtual IP address to be on a different network than the physical IP addresses of the Cluster Members. In this case, you must configure the required static routes on the Cluster Members. See the <a href="#">R80.40 ClusterXL Administration Guide</a>.</p> <ol style="list-style-type: none"> <li>In the <b>Topology</b> section: <ul style="list-style-type: none"> <li>■ Make sure the settings are correct in the <b>Leads To</b> and <b>Security Zone</b> fields.</li> <li>■ Make sure to enable the <b>Anti-Spoofing</b>.</li> </ul> </li> </ol> <p><b>Important:</b></p>  <ul style="list-style-type: none"> <li>■ Make sure the Bridge interface and Bridge slave interfaces are <b>not</b> in the Topology.</li> <li>■ You cannot define the <b>Topology</b> of the Bridge interface. It is <b>External</b> by default.</li> </ul>
11	Click <b>OK</b> .
12	Publish the SmartConsole session.

#### 4. Configure the applicable Security Policies for the ClusterXL in SmartConsole

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

Step	Instructions
3	Create a new policy and configure the applicable layers: <ol style="list-style-type: none"> <li>At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>Click <b>Close</b>.</li> <li>On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>
4	Create the applicable rules in the Access Control and Threat Prevention policies.   <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in " <a href="#">Deploying a Security Gateway or a ClusterXL in Bridge Mode</a> " on page 726.
5	Install the Access Control Policy on the ClusterXL object.
6	Install the Threat Prevention Policy on the ClusterXL object.

## 5. Examine the cluster configuration

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.
2	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: show cluster state</li> <li>■ In the Expert mode, run: cphaprof state</li> </ul> <b>Example output:</b> <pre>Member1&gt; show cluster state  Cluster Mode:  High Availability (Active Up, <b>Bridge Mode</b>) with IGMP Membership  ID      Unique Address  Assigned Load   State      Name 1 (local)  11.22.33.245  100%          ACTIVE    Member1 2           11.22.33.246  100%          ACTIVE    Member2</pre>
3	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> <li>■ In Gaia Clish, run: show cluster members interfaces all</li> <li>■ In the Expansion Line Card, run: cphaprof -a if</li> </ul>

# Accept, or Drop Ethernet Frames with Specific Protocols



**Important** - In a Cluster, you must configure all the Cluster Members in the same way.

By default, Security Gateway and Cluster in Bridge mode *allows* Ethernet frames that carry protocols other than IPv4 (0x0800), IPv6 (0x86DD), or ARP (0x0806) protocols.

Administrator can configure a Security Gateway and Cluster in 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 Security Gateway (each Cluster Member).
2	Log in to the Expert mode.
3	Backup the current /etc/rc.d/init.d/network file: <pre>cp -v /etc/rc.d/init.d/network{,_BKP}</pre>
4	Edit the current /etc/rc.d/init.d/network file: <pre>vi /etc/rc.d/init.d/network</pre>
5	After the line: <pre>./etc/init.d/functions</pre> Add this line: <pre>/sbin/sysctl -w net.bridge.bpdu_forwarding=0</pre>
6	Save the changes in the file and exit the Vi editor.
7	Reboot the Security Gateway (each Cluster Member).
8	Make sure the new configuration is loaded: <pre>sysctl net.bridge_bpdu_forwarding</pre> The output must show: <pre>net.bridge_bpdu_forwarding = 0</pre>

# Routing and Bridge Interfaces

Security Gateways with a Bridge interface can support Layer 3 routing over non-bridged interfaces.

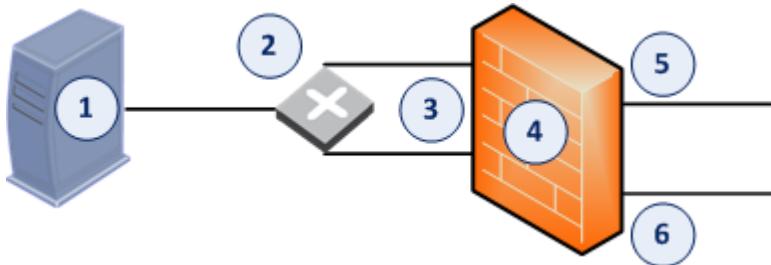
If you configure a Bridge interface with an IP address on a Security Gateway (not on Cluster Members), the Bridge interface functions as a regular Layer 3 interface.

The Bridge interface participates in IP routing decisions on the Security Gateway 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 Gateway can support multiple Bridge interfaces, but only one Bridge interface can have an IP address.
- A Security Gateway cannot filter or transmit packets that it inspected before on a Bridge interface (to avoid double-inspection).

# Managing a Security Gateway through the Bridge Interface

## Example Topology



Item	Description
1	Security Management Server
2	Router
3	Bridge interface on the Security Gateway
4	Security Gateway
5	Regular traffic interface on the Security Gateway
6	Regular traffic interface on the Security Gateway

## Packet flow

1. The Security Management Server sends a management packet to the Management Interface on the Security Gateway.  
This Management Interface is configured as Bridge interface.
2. The Security Gateway inspects the first management packet it receives on the first slave of the Bridge interface.
3. The Security Gateway forwards the inspected management packet to the router through the second slave of the Bridge interface.
4. The router sends the packet to the first slave of the Bridge interface.
5. The Security Gateway concludes that this packet is a retransmission and drops it.

## Procedure

Configure the Security Gateway to reroute packets on the Bridge interface.

Set the value of the kernel parameter "`fwx_bridge_reroute_enabled`" to 1.

The Security Gateway makes sure that the MD5 hash of the packet that leaves the Management Interface and enters the Bridge interface is the same.

Other packets in this connection are handled by the Bridge interface without using the router.

**Notes:**

- To make the change permanent (to survive reboot), you configure the value of the required kernel parameter in the configuration file.  
This change applies only after a reboot.
- To apply the change on-the-fly (does not survive reboot), you configure the value of the required kernel parameter with the applicable command.

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	<p>Modify the \$FWDIR/boot/modules/fw kern.conf file:</p> <p>a. Back up the current \$FWDIR/boot/modules/fw kern.conf file:</p> <pre>cp -v \$FWDIR/boot/modules/fw kern.conf{,_BKP}</pre> <p>If this file does not exist, create it:</p> <pre>touch \$FWDIR/boot/modules/fw kern.conf</pre> <p>b. Edit the current \$FWDIR/boot/modules/fw kern.conf file:</p> <pre>vi \$FWDIR/boot/modules/fw kern.conf</pre> <p>c. Add this line in the file:</p> <pre>fwx_bridge_reroute_enabled=1</pre> <p> <b>Important</b> - This configuration file does <b>not</b> support spaces or comments.</p> <p>d. Save the changes in the file. e. Exit the Vi editor.</p>
4	<p>Set the value of the required kernel parameter on-the-fly:</p> <pre>fw ctl set int fwx_bridge_reroute_enabled 1</pre>
5	<p>Make sure the Security Gateway loaded the new configuration:</p> <pre>fw ctl get int fwx_bridge_reroute_enabled</pre> <p>The output must return</p> <pre>fwx_bridge_reroute_enabled = 1</pre>
6	Reboot the Security Gateway when possible.
7	<p>After the reboot, make sure the Security Gateway loaded the new configuration:</p> <pre>fw ctl get int fwx_bridge_reroute_enabled</pre> <p>The output must return</p> <pre>fwx_bridge_reroute_enabled = 1</pre>

# 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 is permitted regardless of the Rule Base.

This is an example of an explicit Rule Base that permits ICMPv6 Neighbor Discovery protocol:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
IPv6 Neighbor Discovery	Network object that represents the Bridged Network	Network object that represents the Bridged Network	Any	neighbor-advertisement neighbor-solicitation router-advertisement router-solicitation redirect6	Accept	Log	Policy Targets

## Managing Ethernet Protocols

It is possible to configure a Security Gateway with bridge interface to allow or drop protocols that are not based on IP that pass through the bridge interface. For example, protocols that are not IPv4, IPv6, or ARP.

By default, these protocols are allowed by the Security Gateway.

Frames for protocols that are not IPv4, IPv6, or ARP are allowed if:

- On the Security Gateway, the value of the kernel parameter `fwaccept_unknown_protocol` is 1 (all frames are accepted)
- OR in the applicable `user.def` file on the Management Server, the protocol IS defined in the `allowed_ethernet_protocols` table.
- AND in the applicable `user.def` file on the Management Server, the protocol is NOT defined in the `dropped_ethernet_protocols` table.

To configure the Security Gateway to accept only specific protocols that are not IPv4, IPv6, or ARP:

Step	Instructions
1	<p>On the Security Gateway, configure the value of the kernel parameter <code>fwaccept_unknown_protocol</code> to 0.</p> <p> <b>Important</b> - In a Cluster, you must configure all the Cluster Members in the same way.</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Gateway.</li> <li>Log in to the Expert mode.</li> <li>Back up the current <code>\$FWDIR/boot/modules/fw kern.conf</code> file:  <pre>cp -v \$FWDIR/boot/modules/fw kern.conf{,_BKP}</pre> </li> <li>Edit the current <code>\$FWDIR/boot/modules/fw kern.conf</code> file:  <pre>vi \$FWDIR/boot/modules/fw kern.conf</pre> </li> <li>Add this line (spaces or comments are not allowed):  <pre>fwaccept_unknown_protocol=0</pre> </li> <li>Save the changes in the file and exit the editor.</li> <li>Reboot the Security Gateway.  If the reboot is not possible at this time, then: <ul style="list-style-type: none"> <li>Run this command to make the required change:  <pre>fw ctl set int fwaccept_unknown_protocol 0</pre> </li> <li>Run this command to make sure the required change was accepted:  <pre>fw ctl get int fwaccept_unknown_protocol</pre> </li> </ul> </li> </ol>

Step	Instructions
2	<p>On the Management Server, edit the applicable <code>user.def</code> file.</p>  <p><b>Note</b> - For the list of <code>user.def</code> files, see <a href="#">sk98239</a>.</p> <ol style="list-style-type: none"> <li>a. Back up the current applicable <code>user.def</code> file.</li> <li>b. Edit the current applicable <code>user.def</code> file.</li> <li>c. Add these directives: <ul style="list-style-type: none"> <li>■ <code>allowed_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to accept</li> <li>■ <code>dropped_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to drop</li> </ul> </li> </ol> <p><b>Example</b></p> <pre>\$ifndef __user_def__ #define __user_def__  \\ \\ User defined INSPECT code \\  allowed_ethernet_protocols={ &lt;0x0800,0x86DD,0x0806&gt;} ; dropped_ethernet_protocols={ &lt;0x8137,0x8847,0x9100&gt;} ;  endif /*__user_def__*/</pre> <p>For the list of EtherType numbers, see <a href="http://standards-oui.ieee.org/ethertype/eth.csv">http://standards-oui.ieee.org/ethertype/eth.csv</a>.</p> <ol style="list-style-type: none"> <li>d. Save the changes in the file and exit the editor.</li> </ol>
3	In SmartConsole, install the Access Control Policy on this Security Gateway object.

# Configuring Link State Propagation (LSP)

On Check Point Appliances that run as a Security Gateway or ClusterXL Cluster Members, you can bind together in Bridge Mode two physical ports on a Check Point Expansion Line Card.

When the link state for one bridged slave port goes down, the other bridged slave port also goes down.

Switch detects and reacts faster to a link failure on the other side of a bridge or another part of the network.

**Link State Propagation is supported on Check Point Appliances with these Expansion Line Cards:**

Line Card SKU	Description	Driver
CPAC-4-1C	4 Port 10/100/1000 Base-T Ethernet (RJ45) interface card	IGB
CPAC-8-1C	8 Port 10/100/1000 Base-T Ethernet (RJ45) interface card	IGB
CPAC-4-1F	4 Port 1000 Base-F Fiber (SFP) interface card	IGB
CPAC-4-10F	4 Port 10G Base-F Fiber (SFP+) interface card	IXGBE

You can configure the Link State Propagation in one of these modes:

LSP Mode	Description
Automatic port detection and port pair creation	Security Gateways and Cluster Members automatically assign all bridged ports to port pairs.
Manual port pair creation	You manually configure the assignment of bridged ports to port pairs.   <b>Note</b> - You can configure up to four port pairs.

## Important:



- In a Cluster, you must configure all the Cluster Members in the same way.
- Link State Propagation does **not** support Bond interfaces.

## Configuring Link State Propagation for automatic port detection

Step	Instructions
1	Connect to the command line on the Security Gateway or <i>each</i> Cluster Member.
2	Log in to the Expert mode.

Step	Instructions
3	<p>Back up the current \$FWDIR/boot/modules/fw kern.conf file:</p> <pre>cp -v \$FWDIR/boot/modules/fw kern.conf{,_BKP}</pre> <p>If this file does not exist, create it:</p> <pre>touch \$FWDIR/boot/modules/fw kern.conf</pre>
4	<p>Edit the current \$FWDIR/boot/modules/fw kern.conf file:</p> <pre>vi \$FWDIR/boot/modules/fw kern.conf</pre>
5	<p>Add this line:</p> <pre>fw_link_state_propagation_enabled=1</pre>
6	<p>Save the changes in the file and exit the Vi editor.</p>
7	<p>Reboot the Security Gateway or <i>each</i> Cluster Member.</p>
8	<p>Make sure the Security Gateway or Cluster Members loaded the new configuration:</p> <pre>fw ctl get int fw_link_state_propagation_enabled</pre> <p>The returned output must show:</p> <pre>fw_link_state_propagation_enabled = 1</pre>

### Configuring Link State Propagation for manual port detection

Step	Instructions
1	<p>Connect to the command line on the Security Gateway or <i>each</i> Cluster Member.</p>
2	<p>Log in to the Expert mode.</p>
3	<p>Back up the current \$FWDIR/boot/modules/fw kern.conf file:</p> <pre>cp -v \$FWDIR/boot/modules/fw kern.conf{,_BKP}</pre> <p>If this file does not exist, create it:</p> <pre>touch \$FWDIR/boot/modules/fw kern.conf</pre>
4	<p>Edit the current \$FWDIR/boot/modules/fw kern.conf file:</p> <pre>vi \$FWDIR/boot/modules/fw kern.conf</pre>

Step	Instructions
5	<p>Add these lines (you can configure up to four LSP pairs):</p> <pre>fw_link_state_propagation_enabled=1 fw_manual_link_state_propagation_enabled=1 fw_lsp_pair1=&lt;interface_name_1,interface_name_2&gt; fw_lsp_pair2=&lt;interface_name_3,interface_name_4&gt; fw_lsp_pair3=&lt;interface_name_5,interface_name_6&gt; fw_lsp_pair4=&lt;interface_name_7,interface_name_8&gt;</pre>
	<p><b>Example:</b></p> <pre>fw_lsp_pair1="eth1,eth2" fw_lsp_pair2="eth3,eth4"</pre>
6	Save the changes in the file and exit the Vi editor.
7	Reboot the Security Gateway or <i>each</i> Cluster Member.

Step	Instructions
8	<p>Make sure the Security Gateway or Cluster Members loaded the new configuration:</p> <ul style="list-style-type: none"> <li>a. Output of this command  <pre>fw ctl get int fw_link_state_propagation_enabled</pre> <p>must return</p> <pre>fw_link_state_propagation_enabled = 1</pre> </li> <li>b. Output of this command  <pre>fw ctl get int fw_manual_link_state_propagation_enabled</pre> <p>must return</p> <pre>fw_manual_link_state_propagation_enabled = 1</pre> </li> <li>c. Output of this command  <pre>fw ctl get str fw_lsp_pair1</pre> <p>must return the names of the interfaces configured in this pair</p> <pre>&lt;interface_name_1, interface_name_2&gt;</pre> </li> <li>d. Output of this command  <pre>fw ctl get str fw_lsp_pair2</pre> <p>must return the names of the interfaces configured in this pair</p> <pre>&lt;interface_name_3, interface_name_4&gt;</pre> </li> <li>e. Output of this command  <pre>fw ctl get str fw_lsp_pair3</pre> <p>must return the names of the interfaces configured in this pair</p> <pre>&lt;interface_name_5, interface_name_6&gt;</pre> </li> <li>f. Output of this command  <pre>fw ctl get str fw_lsp_pair4</pre> <p>must return the names of the interfaces configured in this pair</p> <pre>&lt;interface_name_7, interface_name_8&gt;</pre> </li> </ul>

#### For more information:

See [sk108121: How to configure Link State Propagation \(LSP\) in a Bridge interface on Gaia OS and SecurePlatform OS](#).

# Security Before Firewall Activation

To protect the Security Gateway and network, Check Point Security Gateway has baseline security:

Baseline Security	Name of Policy	Description
Boot Security	defaultfilter	Security during boot process.
Initial Policy	InitialPolicy	Security before a policy is installed for the first time, or when Security Gateway failed to load the policy.



**Important** - If you disable the boot security or unload the currently installed policy, you leave your Security Gateway, or a Cluster Member without protection.



**Best Practice** - Before you disable the boot security, we recommend to disconnect your Security Gateway, or a Cluster Member from the network completely.

For additional information, see these commands in the [R80.40 CLI Reference Guide](#):

Command	Description
\$CPDIR/bin/cpstat -f policy fw	Shows the currently installed policy
\$FWDIR/bin/control_bootsec {-r   -R}	Disables the boot security
\$FWDIR/bin/control_bootsec [-g   -G]	Enables the boot security
\$FWDIR/bin/comp_init_policy [-u   -U]	Deletes the local state policy
\$FWDIR/bin/comp_init_policy [-g   -G]	Creates the local state Initial Policy
\$FWDIR/bin/fw unloadlocal	Unloads the currently installed policy

# Boot Security

The Boot Security protects the Security Gateway and its networks, during the boot:

- Disables the IP Forwarding in Linux OS kernel
- Loads the Default Filter Policy



**Important** - In a Cluster, you must configure all the Cluster Members in the same way.

## The Default Filter Policy

The Default Filter Policy (`defaultfilter`) protects the Security Gateway from the time it boots up until it installs the user-defined Security Policy.

Boot Security disables IP Forwarding and loads the Default Filter Policy.

There are three Default Filters templates on the Security Gateway:

Default Filter Mode	Default Filter Policy File	Description
Boot Filter	<code>\$FWDIR/lib/defaultfilter.boot</code>	<p>This filter:</p> <ul style="list-style-type: none"> <li>■ Drops all incoming packets that have the same source IP addresses as the IP addresses assigned to the Security Gateway interfaces</li> <li>■ Allows all outbound packets from the Security Gateway</li> </ul>
Drop Filter	<code>\$FWDIR/lib/defaultfilter.drop</code>	<p>This filter drops all inbound <i>and</i> outbound packets on the Security Gateway.</p> <p> <b>Best Practice</b> - If the boot process requires that the Security Gateway communicate with other hosts, do <b>not</b> use the <i>Drop Filter</i>.</p>

Default Filter Mode	Default Filter Policy File	Description
Filter for Dynamically Assigned Gateways (DAG)	\$FWDIR/lib/defaultfilter.dag	<p>This filter for Security Gateways with Dynamically Assigned IP address:</p> <ul style="list-style-type: none"> <li>■ Allows all DHCP Requests</li> <li>■ Allows all DHCP Replies</li> <li>■ Uses Boot Filter:           <ul style="list-style-type: none"> <li>a. Drops all incoming packets that have the same source IP addresses as the IP addresses assigned to the Security Gateway interfaces</li> <li>b. Allows all outbound packets from the Security Gateway</li> </ul> </li> </ul>

## Selecting the Default Filter Policy

Step	Instructions
1	Make sure to configure and install a Security Policy on the Security Gateway.
2	Connect to the command line on the Security Gateway.
3	Log in to the Expert mode.
4	Back up the current Default Filter Policy file: <pre>cp -v \$FWDIR/conf/defaultfilter.pf{,_BKP}</pre>
5	Create a new Default Filter Policy file. <ul style="list-style-type: none"> <li>■ To create a new Boot Filter, run:  <pre>cp -v \$FWDIR/lib/defaultfilter.boot \$FWDIR/conf/defaultfilter.pf</pre> </li> <li>■ To create a new Drop Filter, run:  <pre>cp -v \$FWDIR/lib/defaultfilter.drop \$FWDIR/conf/defaultfilter.pf</pre> </li> <li>■ To create a new DAG Filter, run:  <pre>cp -v \$FWDIR/lib/defaultfilter.dag \$FWDIR/conf/defaultfilter.pf</pre> </li> </ul>

Step	Instructions
6	<p>Compile the new Default Filter file:</p> <pre>fw defaultgen</pre> <ul style="list-style-type: none"> <li>■ The new compiled Default Filter file for IPv4 traffic is:</li> </ul> <pre>\$FWDIR/state/default.bin</pre> <ul style="list-style-type: none"> <li>■ The new compiled Default Filter file for IPv6 traffic is:</li> </ul> <pre>\$FWDIR/state/default.bin6</pre>
7	<p>Get the path of the Default Filter Policy file:</p> <pre>\$FWDIR/boot/fwboot bootconf get_def</pre> <p><b>Example:</b></p> <pre>[Expert@MyGW:0]# \$FWDIR/boot/fwboot bootconf get_def /etc/fw.boot/default.bin [Expert@MyGW:0]#</pre>
8	<p>Copy new compiled Default Filter file to the path of the Default Filter Policy file.</p> <ul style="list-style-type: none"> <li>■ For IPv4 traffic, run:</li> </ul> <pre>cp -v \$FWDIR/state/default.bin /etc/fw.boot/default.bin</pre> <ul style="list-style-type: none"> <li>■ For IPv6 traffic, run:</li> </ul> <pre>cp -v \$FWDIR/state/default.bin6 /etc/fw.boot/default.bin6</pre>
9	<p>Make sure to connect to the Security Gateway over a serial console.</p> <p> <b>Important</b> - If the new Default Filter Policy fails and blocks all access through the network interfaces, you can unload that Default Filter Policy and install the working policy.</p>
10	Reboot the Security Gateway.

## Defining a Custom Default Filter

Administrators with Check Point INSPECT language knowledge can define customized Default Filters.



**Important** - Make sure your customized Default Filter policy does not interfere with the Security Gateway boot process.

Step	Instructions
1	Make sure to configure and install a Security Policy on the Security Gateway.
2	Connect to the command line on the Security Gateway.

Step	Instructions
3	Log in to the Expert mode.
4	<p>Back up the current Default Filter Policy file:</p> <pre data-bbox="362 332 1049 366">cp -v \$FWDIR/conf/defaultfilter.pf{,_BKP}</pre>
5	<p>Create a new Default Filter Policy file.</p> <ul style="list-style-type: none"> <li>■ To use the Boot Filter as a template, run:</li> <pre data-bbox="441 512 1033 568">cp -v \$FWDIR/lib/defaultfilter.boot \$FWDIR/conf/defaultfilter.pf</pre> <li>■ To use the Drop Filter as a template, run:</li> <pre data-bbox="441 640 1033 696">cp -v \$FWDIR/lib/defaultfilter.drop \$FWDIR/conf/defaultfilter.pf</pre> <li>■ To use the DAG Filter as a template, run:</li> <pre data-bbox="441 768 1017 824">cp -v \$FWDIR/lib/defaultfilter.dag \$FWDIR/conf/defaultfilter.pf</pre> </ul>
6	<p>Edit the new Default Filter Policy file to include the applicable INSPECT code.</p> <p><b>Important</b> - Your customized Default Filter must not use these functions:</p>  <ul style="list-style-type: none"> <li>■ Logging</li> <li>■ Authentication</li> <li>■ Encryption</li> <li>■ Content Security</li> </ul>
7	<p>Compile the new Default Filter file:</p> <pre data-bbox="362 1253 584 1282">fw defaultgen</pre> <ul style="list-style-type: none"> <li>■ The new compiled Default Filter file for IPv4 traffic is:</li> <pre data-bbox="441 1354 847 1383">\$FWDIR/state/default.bin</pre> <li>■ The new compiled Default Filter file for IPv6 traffic is:</li> <pre data-bbox="441 1455 867 1484">\$FWDIR/state/default.bin6</pre> </ul>
8	<p>Get the path of the Default Filter Policy file:</p> <pre data-bbox="362 1596 954 1626">\$FWDIR/boot/fwboot bootconf get_def</pre> <p>Example:</p> <pre data-bbox="362 1697 1240 1799">[Expert@MyGW:0]# \$FWDIR/boot/fwboot bootconf get_def /etc/fw.boot/default.bin [Expert@MyGW:0]#</pre>

Step	Instructions
9	<p>Copy new complied Default Filter file to the path of the Default Filter Policy file.</p> <ul style="list-style-type: none"> <li>■ For IPv4 traffic, run:</li> </ul> <pre>cp -v \$FWDIR/state/default.bin /etc/fw.boot/default.bin</pre> <ul style="list-style-type: none"> <li>■ For IPv6 traffic, run:</li> </ul> <pre>cp -v \$FWDIR/state/default.bin6 /etc/fw.boot/default.bin6</pre>
10	<p>Make sure to connect to the Security Gateway over a serial console.</p> <p> <b>Important</b> - If the new Default Filter Policy fails and blocks all access through the network interfaces, you can unload that Default Filter Policy and install the working policy.</p>
11	Reboot the Security Gateway.

## Using the Default Filter Policy for Maintenance

It is sometimes necessary to stop the Security Gateway for maintenance. It is not always practical to disconnect the Security Gateway from the network (for example, if the Security Gateway is on a remote site).

To stop the Security Gateway for maintenance and maintain security, you can run:

Command	Description
<pre>cpstop - fwflag - default</pre>	<ul style="list-style-type: none"> <li>■ Shuts down Check Point processes</li> <li>■ Loads the Default Filter policy (<code>defaultfilter</code>)</li> </ul>
<pre>cpstop - fwflag - proc</pre>	<ul style="list-style-type: none"> <li>■ Shuts down Check Point processes</li> <li>■ Keeps the currently loaded kernel policy</li> <li>■ Maintains the Connections table, so that after you run the <code>cpstart</code> command, you do not experience dropped packets because they are "out of state"</li> </ul> <p> <b>Note</b> - Only security rules that do not use user space processes continue to work.</p>

# The Initial Policy

Until the Security Gateway administrator installs the Security Policy on the Security Gateway for the first time, security is enforced by an Initial Policy.

The Initial Policy operates by adding the predefined implied rules to the Default Filter policy.

These implied rules forbid most communication, yet allow the communication needed for the installation of the Security Policy.

The Initial Policy also protects the Security Gateway during Check Point product upgrades, when a SIC certificate is reset on the Security Gateway, or in the case of a Check Point product license expiration.



**Note** - During a Check Point upgrade, a SIC certificate reset, or license expiration, the Initial Policy overwrites the user-defined policy.

The sequence of actions during boot of the Security Gateway until a Security Policy is loaded for the first time:

Step	Instructions
1	The Security Gateway boots up.
2	The Security Gateway disables IP Forwarding and loads the Default Filter policy.
3	The Security Gateway configures the interfaces.
4	The Security Gateway services start.
5	The Security Gateway fetches the Initial Policy from the local directory.
6	Administrator installs the user-defined Security Policy from the Management Server.

The Security Gateway enforces the Initial Policy until administrator installs a user-defined policy.

In subsequent boots, the Security Gateway loads the user-defined policy immediately after the Default Filter policy.

There are different Initial Policies for Standalone and distributed setups:

- In a Standalone configuration, where the Security Management Server and the Security Gateway are on the same computer, the Initial Policy allows CPMI management communication only.

This permits SmartConsole clients to connect to the Security Management Server.

- In a distributed configuration, where the Security Management Server is on one computer and the Security Gateway is on a different computer, the Initial Policy:

- Allows the **cpd** and **fwd** daemons to communicate for SIC (to establish trust) and for Policy installation.
- Does not allow CPMI connections through the Security Gateway.

The SmartConsole is not be able to connect to the Security Management Server, if the SmartConsole must access the Security Management Server through a Security Gateway with the Initial Policy.

# Troubleshooting: Cannot Complete Reboot

In some configurations, the Default Filter policy prevents the Security Gateway from completing the reboot after installation.

Firstly, look at the Default Filter. Does the Default Filter allow traffic required by the boot procedures?

Secondly, if the boot process cannot finish successfully, remove the Default Filter:

Step	Instructions
1	Connect to the Security Gateway over serial console.
2	Reboot the Security Gateway.
3	During boot, press any key to enter the Boot Menu.
4	Select the <b>Start in maintenance mode</b> .
5	Enter the Expert mode password.
6	Set the Default Filter to not load again: <ol style="list-style-type: none"> <li>Go to the \$FWDIR directory:  <pre>cd /opt/CPsuite-&lt;VERSION&gt;/fw1/</pre> </li> <li>Set the Default Filter to not load again:  <pre>./fwboot bootconf set_def</pre> </li> </ol>
7	In the \$FWDIR/boot/boot.conf file, examine the value of the "DEFAULT_FILTER_PATH": <ol style="list-style-type: none"> <li>Go to the \$FWDIR directory:  <pre>cd /opt/CPsuite-&lt;VERSION&gt;/fw1/</pre> </li> <li>examine the value of the "DEFAULT_FILTER_PATH":  <pre>grep DEFAULT_FILTER_PATH boot/boot.conf</pre> </li> </ol>
8	Reboot the Security Gateway.

# Working with Licenses

You can manage licenses on your Security Gateways in these ways:

- In SmartConsole you can activate your licenses. See "["Viewing Licenses in SmartConsole" on page 792](#)".
- In Gaia Portal, you can activate, add, or delete your licenses. See "["Managing Licenses in the Gaia Portal" on page 798](#)".
- In Gaia Clish or the Expert mode, you can add or delete your licenses with the "cplic" command. See the [R80.40 CLI Reference Guide](#) > Chapter *Security Gateway Commands* > Section *cplic*.
- When Security Gateways are **not** connected to the Internet, you can add, delete, attach, and detach your licenses in SmartUpdate. See "["Using Legacy SmartUpdate" on page 801](#)".

When Security Gateways *are* connected to the Internet, they are able to get and update their licenses and contracts without SmartUpdate.

# Viewing Licenses in SmartConsole

## Viewing license information

Step	Instructions
1	In SmartConsole, from the left navigation panel, click <b>Gateways &amp; Servers</b> .
2	From the <b>Columns</b> drop-down list, select <b>Licenses</b> .

You can see these columns:

Column	Instructions
<b>License Status</b>	The general state of the Software Blade licenses: <ul style="list-style-type: none"> <li>■ <b>OK</b> - All the blade licenses are valid.</li> <li>■ <b>Not Activated</b> - Blade licenses are not installed. This is only possible in the first 15 days after the establishment of the SIC with the Security Management Server. After the initial 15 days, the absence of licenses will result in the blade error message.</li> <li>■ <b>Error with &lt;number&gt; blade(s)</b> - The specified number of blade licenses are not installed or not valid.</li> <li>■ <b>Warning with &lt;number&gt; blade(s)</b> - The specified number of blade licenses have warnings.</li> <li>■ <b>N/A</b> - The license information is not available.</li> </ul>
<b>CK</b>	Unique Certificate Key of the license instance.
<b>SKU</b>	Catalog ID from the Check Point User Center.
<b>Account ID</b>	User's account ID.
<b>Support Level</b>	Check Point level of support.
<b>Support Expiration</b>	Date when the Check Point support contract expires.

## Viewing license information for each Software Blade

Step	Instructions
1	Select a Security Gateway or a Security Management Server.

Step	Instructions
2	<p>In the <b>Summary</b> tab below, click the object's <b>License Status</b> (for example: <b>OK</b>). The <b>Device &amp; License Information</b> window opens. It shows basic object information and <b>License Status</b>, license <b>Expiration Date</b>, and important quota information (in the <b>Additional Info</b> column) for each Software Blade.</p> <p><b>Notes:</b></p>  <ul style="list-style-type: none"> <li>■ Quota information, quota-dependent license statuses, and blade information messages are only supported for R80 and above.</li> <li>■ The tooltip of the SKU is the product name.</li> </ul>

The possible values for the Software Blade **License Status** are:

Status	Instructions
<b>Active</b>	The Software Blade is active and the license is valid.
<b>Available</b>	The Software Blade is not active, but the license is valid.
<b>No License</b>	The Software Blade is active, but the license is not valid.
<b>Expired</b>	The Software Blade is active, but the license expired.
<b>About to Expire</b>	The Software Blade is active, but the license will expire in 30 days (default) or less (7 days or less for an evaluation license).
<b>Quota Exceeded</b>	The Software Blade is active, and the license is valid, but the quota of related objects (Security Gateways, files, Virtual Systems, and so on, depending on the blade) is exceeded.
<b>Quota Warning</b>	The Software Blade is active, and the license is valid, but the number of objects of this blade is 90% (default) or more of the licensed quota.
<b>N/A</b>	The license information is not available.

# Monitoring Licenses in SmartConsole

To keep track of license issues, you can use these options in SmartConsole:

Option	Instructions
<b>License Status view</b>	To see and export license information for Software Blades on each specific Security Management Server, Security Gateway, or Log Server object.
<b>License Status report</b>	To see filter and export license status information for all configured Security Management Server, Security Gateway, or Log Server objects.
<b>License Inventory report</b>	To see filter and export license information for Software Blades on all configured Security Management Server, Security Gateway, or Log Server objects.

The **SmartEvent** Software Blade lets you customize the **License Status** and **License Inventory** information from the **Logs & Monitor** view of SmartConsole.

It is also possible to view license information from the **Gateways & Servers** view of SmartConsole without enabling the **SmartEvent** Software Blade on Security Management Server.

The **Gateways & Servers** view in SmartConsole lets you view, filter, and export different license reports:

## The "License Inventory" report

The **Gateways & Servers** view in SmartConsole lets you view and export the **License Inventory** report.

### Viewing the License Inventory report

Step	Instructions
1	In SmartConsole, from the left navigation panel, click <b>Gateways &amp; Servers</b> .
2	From the top toolbar, click <b>Actions &gt; License Report</b> .
3	Wait for the <b>SmartView</b> to load and show this report. By default, this report contains: <ul style="list-style-type: none"> <li>■ <i>Inventory</i> page:               <ul style="list-style-type: none"> <li>• Blade Names</li> <li>• Devices Names</li> <li>• License Statuses</li> </ul> </li> <li>■ <i>License by Device</i> page:               <ul style="list-style-type: none"> <li>• Devices Names</li> <li>• License statuses</li> <li>• CK</li> <li>• SKU</li> <li>• Account ID</li> <li>• Support Level</li> <li>• Next Expiration Date</li> </ul> </li> </ul>

## Exporting the License Inventory report

Step	Instructions
1	In the top right corner, click the <b>Options</b> button.
2	Select the applicable export option - <b>Export to Excel</b> , or <b>Export to PDF</b> .

## The "License Status" report

The **Logs & Monitor** view in SmartConsole lets you view, filter, and export the **License Status** report.

### Viewing the License Status report

Step	Instructions
1	In SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
2	At the top, open a new tab by clicking <b>New Tab</b> , or <b>[+]</b> .
3	In the left section, click <b>Views</b> .
4	In the list of reports, double-click <b>License Status</b> .
5	<p>Wait for the <b>SmartView</b> to load and show this report.          By default, this report contains:</p> <ul style="list-style-type: none"> <li>■ Names of the configured objects</li> <li>■ License status for each object</li> <li>■ CK</li> <li>■ SKU</li> <li>■ Account ID</li> <li>■ Support Level</li> <li>■ Next Expiration Date</li> </ul>

### Filtering the License Status report

Step	Instructions
1	<p>In the top right corner, click the <b>Options</b> button &gt; click <b>View Filter</b>.          The <b>Edit View Filter</b> window opens.</p>
2	<p>Select a <b>Field</b> to filter results.          For example, <b>Device Name</b>, <b>License Status</b>, <b>Account ID</b>.</p>
3	Select the logical operator - <b>Equals</b> , <b>Not Equals</b> , or <b>Contains</b> .
4	Select or enter a filter value.
	 <b>Note</b> - Click the X icon to delete a filter.

Step	Instructions
5	Optional: Click the <b>+</b> icon to configure additional filters.
6	Click <b>OK</b> to apply the configured filters. The report is filtered based on the configured filters.

## Exporting the License Status report

Step	Instructions
1	In the top right corner, click the <b>Options</b> button.
2	Select the applicable export option - <b>Export to Excel</b> , or <b>Export to PDF</b> .

## The "License Inventory" report

The **Logs & Monitor** view in SmartConsole lets you view, filter, and export the **License Inventory** report.

### Viewing the License Inventory report

Step	Instructions
1	In SmartConsole, from the left navigation panel, click <b>Logs &amp; Monitor</b> .
2	At the top, open a new tab by clicking <b>New Tab</b> , or <b>[+]</b> .
3	In the left section, click <b>Reports</b> .
4	In the list of reports, double-click <b>License Inventory</b> .
5	Wait for the <b>SmartView</b> to load and show this report. By default, this report contains: <ul style="list-style-type: none"> <li>■ <i>Inventory</i> page:               <ul style="list-style-type: none"> <li>• Blade Names</li> <li>• Devices Names</li> <li>• License Statuses</li> </ul> </li> <li>■ <i>License by Device</i> page:               <ul style="list-style-type: none"> <li>• Devices Names</li> <li>• License statuses</li> <li>• CK</li> <li>• SKU</li> <li>• Account ID</li> <li>• Support Level</li> <li>• Next Expiration Date</li> </ul> </li> </ul>

## Filtering the License Inventory report

Step	Instructions
1	In the top right corner, click the <b>Options</b> button > click <b>Report Filter</b> . The <b>Edit Report Filter</b> window opens.
2	Select a <b>Field</b> to filter results. For example, <b>Blade Name</b> , <b>Device Name</b> , <b>License Overall Status</b> , <b>Account ID</b> .
3	Select the logical operator - <b>Equals</b> , <b>Not Equals</b> , or <b>Contains</b> .
4	Select or enter a filter value.   <b>Note</b> - Click the <b>X</b> icon to delete a filter.
5	Optional: Click the <b>+</b> icon to configure additional filters.
6	Click <b>OK</b> to apply the configured filters. The report is filtered based on the configured filters.

## Exporting the License Inventory report

Step	Instructions
1	In the top right corner, click the <b>Options</b> button.
2	Select the applicable export option - <b>Export to Excel</b> , or <b>Export to PDF</b> .

# Managing Licenses in the Gaia Portal



**Note** - If it is necessary to get a license, visit the [User Center](#).

## Adding a license

Step	Instructions
1	In the navigation tree, click <b>Maintenance &gt; Licenses</b> .
2	Click <b>New</b> . The <b>Add License</b> window opens.
3	Enter the license data manually, or click <b>Paste License</b> to enter the data automatically.  <b>Note</b> - The <b>Paste License</b> button only shows in Internet Explorer. For other web browsers, paste the license strings into the empty text field.
4	Click <b>OK</b> .

## Deleting a license

Step	Instructions
1	In the navigation tree, click <b>Maintenance &gt; Licenses</b> .
2	Select a license in the table.
3	Click <b>Delete</b> .

# Migrating a License to a New IP Address

Check Point licenses are issued for the main IP address of Check Point computers.

If you change the IP address of your Check Point computer, or if you migrated the management database between the servers with different IP addresses, you must update the applicable configuration.

## Procedure for a Security Management Server

Step	Instructions
1	Connect to your <a href="#">User Center</a> account.
2	Issue a new license for the new IP address.
3	Install the new license (issued for the new IP address) on your Security Management Server.
4	Remove the old license (issued for the old IP address) from your Security Management Server.
5	Restart Check Point Services: <pre>cpstop cpstart</pre>
6	In SmartConsole: 1. Connect with SmartConsole to the (Primary) Security Management Server. 2. Open the Security Management Server object. 3. In the left tree, click <b>Network Management</b> . 4. Make sure to update the IP Address and topology. 5. Click <b>OK</b> . 6. Publish the SmartConsole session. 7. Install the database: a. In the top left corner, click <b>Menu &gt; Install database</b> . b. Select all objects. c. Click <b>Install</b> . d. Click <b>OK</b> .
7	On your DNS Server, map the host name of your Security Management Server to the new IP address.

## Procedure for a Multi-Domain Server or Multi-Domain Log Server

Step	Instructions
1	Connect to your <a href="#">User Center</a> account.
2	Issue a new license for the new IP address.
3	Install the new license (issued for the new IP address) on your Multi-Domain Server or Multi-Domain Log Server.

Step	Instructions
4	Remove the old license (issued for the old IP address) from your Multi-Domain Server or Multi-Domain Log Server.
5	Change the Leading Interface. See " <a href="#">Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server</a> " on page 681.
6	On your DNS Server, map the host name of your Multi-Domain Server or Multi-Domain Log Server to the new IP address.

### Procedure for dedicated Log Servers and dedicated SmartEvent Servers

Step	Instructions
1	Connect to your <a href="#">User Center</a> account.
2	Issue a new license for the new IP address.
3	Install the new license (issued for the new IP address) on your Log Server or SmartEvent Server.
4	Remove the old license (issued for the old IP address) from your Log Server or SmartEvent Server.
5	Restart Check Point Services: <pre>cpstop cpstart</pre>
6	In SmartConsole: <ol style="list-style-type: none"> <li>1. Connect with SmartConsole to the applicable Management Server that manages your dedicated Log Server or SmartEvent Server.</li> <li>2. Open the object of your dedicated Log Server or SmartEvent Server.</li> <li>3. In the left tree, click <b>Network Management</b>.</li> <li>4. Make sure to update the IP Address and topology.</li> <li>5. Click <b>OK</b>.</li> <li>6. Publish the SmartConsole session.</li> <li>7. Install the database:           <ol style="list-style-type: none"> <li>a. In the top left corner, click <b>Menu &gt; Install database</b>.</li> <li>b. Select all objects.</li> <li>c. Click <b>Install</b>.</li> <li>d. Click <b>OK</b>.</li> </ol> </li> <li>8. Install the Access Control Policy on all managed Security Gateways that send their logs to your dedicated Log Server or SmartEvent Server.</li> </ol>
7	On your DNS Server, map the host name of your dedicated Log Server or SmartEvent Server to the new IP address.

# Using Legacy SmartUpdate

When Security Gateways are **not** connected to the Internet, you can add, delete, attach, and detach your licenses in SmartUpdate.

When Security Gateways *are* connected to the Internet, they are able to get and update their licenses and contracts without SmartUpdate.

SmartUpdate distributes licenses and software packages for managed Check Point and OPSEC Certified products.

SmartUpdate provides a centralized way to guarantee that Internet security throughout the enterprise network is always up to date.

These features and tools are available in SmartUpdate:

- Maintaining licenses
- Upgrading packages for R77.30 and below
- Adding packages to Package Repository for R77.30 and below

**Important:**



- The SmartUpdate GUI shows two tabs - **Package Management** and **Licenses & Contracts**.
- For versions R80.10 and above, the tools in the **Package Management** tab are *no longer supported*.
- To install packages on Gaia OS, use CPUSE (see [sk92449](#)), or Central Deployment Tool (see [sk111158](#)).

For further information, see "*Installing Software Packages on Gaia*" on page 160.

# Accessing SmartUpdate

Step	Instructions
1	<p>Open the SmartUpdate in one of these ways:</p> <ul style="list-style-type: none"><li>■ In SmartConsole, in the top left corner, click <b>Menu &gt; Manage licenses &amp; packages</b>.</li><li>■ On the SmartConsole client, run this executable file directly:<ul style="list-style-type: none"><li>• On Windows OS 32-bit:<pre>C:\Program Files\CheckPoint\ SmartConsole\&lt;<i>Rxx</i>&gt;\PROGRAM\SmartDistributor.exe</pre></li><li>• On Windows OS 64-bit:<pre>C:\Program Files (x86)\CheckPoint\ SmartConsole\&lt;<i>Rxx</i>&gt;\PROGRAM\SmartDistributor.exe</pre></li></ul></li></ul>
2	<p>In the top left corner, click <b>Menu &gt; View &gt; Menu Bar</b>. The menu names appear at the top of the GUI.</p>

# Licenses Stored in the Licenses & Contracts Repository

When you add a license with SmartUpdate, it is stored in the **Licenses & Contracts Repository**.

The SmartUpdate provides a global view of all licenses available and all of the assigned licenses.

To activate the license once it is in the Repository, it has to be attached to a Security Gateway and registered with the Management Server.

There are two license types available:

License Type	Instructions
Central	<p>The Central license is the preferred method of licensing.</p> <ul style="list-style-type: none"><li>■ A Central license is tied to the IP address of the Management Server.</li><li>■ There is one IP address for all licenses.</li><li>■ The license remains valid if you change the IP address of the Security Gateway.</li><li>■ A license can be moved from one Check Point Security Gateway to another easily.</li><li>■ Maximum flexibility.</li></ul>
Local	<p>The Local license is an older method of licensing that is still supported.</p> <ul style="list-style-type: none"><li>■ A Local license is tied to the IP address of the specific Security Gateway.</li><li>■ Cannot be transferred to a Security Gateway with a different IP address.</li></ul>

# Licensing Terms for SmartUpdate

Term	Instructions
Add	<p>You can add any license that you receive from the <a href="#">User Center</a> to the <b>Licenses &amp; Contracts Repository</b>.</p> <ul style="list-style-type: none"> <li>■ You can add the licenses directly from a User Center account.</li> <li>■ You can add the licenses from a file that you receive from the User Center.</li> <li>■ You can add the licenses manually by pasting or typing the license details.</li> </ul> <p>When you add the Local license to the <b>Licenses &amp; Contracts Repository</b>, it also attaches it to the Security Gateway with the IP address, for which the license was issued.</p> <p>See "<a href="#">Adding New Licenses to the Licenses &amp; Contracts Repository</a>" on page 807.</p>
Attach	<p>You can attach a license from the <b>Licenses &amp; Contracts Repository</b> to a managed Security Gateway.</p> <p>See "<a href="#">Attaching a License to a Security Gateway</a>" on page 810.</p>
Detach	<p>When you detach a license from a managed Security Gateway, you have to uninstall the license from that Security Gateway.</p> <p>If this is a Central license, this operation makes that license in the <b>Licenses &amp; Contracts Repository</b> available to other managed Security Gateways.</p> <p>See "<a href="#">Detaching a License from a Security Gateway</a>" on page 811.</p>
Get	<p>You can add information from your managed Security Gateways about the licenses you installed locally.</p> <p>This updates the <b>Licenses &amp; Contracts Repository</b> with all local licenses across the installation.</p> <p>The Get operation is a two-way process that places all locally installed licenses in the <b>License &amp; Contract Repository</b> and removes all locally deleted licenses from the <b>Licenses &amp; Contracts Repository</b>.</p> <p>See "<a href="#">Getting Licenses from Security Gateways</a>" on page 812.</p>
Delete	<p>You can delete a license from the <b>Licenses &amp; Contracts Repository</b>.</p> <p>See "<a href="#">Deleting a License from the Licenses &amp; Contracts Repository</a>" on page 809.</p>
Export	<p>You can export a license from the <b>Licenses &amp; Contracts Repository</b> to a file.</p> <p>See "<a href="#">Exporting a License to a File</a>" on page 813.</p>
License Expiration	<p>Licenses expire on a particular date, or never.</p> <p>If a license expires, the applicable products and features stop working on the Check Point computer, to which the license is attached.</p> <p>See "<a href="#">Checking for Expired Licenses</a>" on page 814.</p>

Term	Instructions
<b>State</b>	<p>The license state depends on whether the license is associated with a managed Security Gateway in the <b>Licenses &amp; Contracts Repository</b>, and whether the license is installed on that Security Gateway.</p> <p>The license state definitions are:</p> <ul style="list-style-type: none"> <li>■ <b>Attached</b> - Indicates that the license is associated with a managed Security Gateway in the <b>Licenses &amp; Contracts Repository</b>, and is installed on that Security Gateway.</li> <li>■ <b>Unattached</b> - Indicates that the license is not associated with managed Security Gateways in the <b>Licenses &amp; Contracts Repository</b>, and is not installed on managed Security Gateways.</li> <li>■ <b>Assigned</b> Indicates that the license that is associated with a managed Security Gateway in the <b>Licenses &amp; Contracts Repository</b>, but has not yet been installed on a Security Gateway.</li> </ul>
<b>Upgrade Status</b>	This is a field in the <b>Licenses &amp; Contracts Repository</b> that contains an error message from the User Center when the License Upgrade process fails.
<b>Central License</b>	Attach a <b>Central License</b> to the IP address of your Management Server.
<b>Local License</b>	A <b>Local License</b> is tied to the IP address of the specific Security Gateway. You can only use a local license with a Security Gateway or a Security Management Server with the same address.
<b>Multi-License File</b>	This is a license file that contains more than one license. The "cplic put" and "cplic add" commands support these files.
<b>Certificate Key</b>	This is a string of 12 alphanumeric characters. This number is unique to each package.
<b>Features</b>	This is a character string that identifies the features of a package.
<b>cplic</b>	A CLI utility to manage local licenses on Check Point computers. For details, see the <a href="#">R80.40 CLI Reference Guide</a> - Chapter <i>Security Management Server Commands</i> - Section <i>cplic</i> .

# Viewing the Licenses & Contracts Repository

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click the <b>Licenses &amp; Contracts</b> tab.

# Adding New Licenses to the Licenses & Contracts Repository

To install a license, you must first add it to the **Licenses & Contracts Repository**.

You can add any license that you receive from the [User Center](#) to the Licenses & Contracts Repository.

- You can add the licenses directly from a User Center account.
- You can add the licenses from a file that you receive from the User Center.
- You can add the licenses manually by pasting or typing the license details.

## Notes:



- Unattached Central licenses appear in the **Licenses & Contracts Repository**.
- When you add the Local license to the **Licenses & Contracts Repository**, the Management Server attaches it to the Security Gateway with the IP address, for which the license was issued.
- All licenses are assigned a default name in the format <SKU>@<Time Date>, which you can modify later.

## Adding a license directly from a User Center account

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click <b>Licenses &amp; Contracts</b> tab.
3	Click <b>Licenses &amp; Contracts</b> menu at the top > <b>Add License</b> > <b>From User Center</b> .
4	Enter your User Center credentials.
5	Click <b>Assets / Info</b> > <b>Product Center</b> .
6	Perform one of the following: <ul style="list-style-type: none"> <li>■ Generate a new license, if there are no identical licenses. This adds the license to the <b>Licenses &amp; Contracts Repository</b>.</li> <li>■ Change the IP address of an existing license with <b>Move IP</b>.</li> <li>■ Change the license from Local to Central.</li> </ul>

## Adding a license from a file

Step	Instructions
1	In the applicable <a href="#">User Center</a> account: <ol style="list-style-type: none"> <li>1. Generate a license.</li> <li>2. Click the <b>License Information</b> tab.</li> <li>3. Click the <b>Get Last License</b>.</li> <li>4. Click the <b>Get License File</b>.</li> <li>5. Save the <b>CPLicenseFile.lic</b> file.</li> </ol>
2	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
3	Click the <b>Licenses &amp; Contracts</b> tab.
4	Click the <b>Licenses &amp; Contracts</b> menu at the top > <b>Add License &gt; From File</b> .
5	Locate and select the downloaded <b>CPLicenseFile.lic</b> file.
6	Click <b>Open</b> .
7	Follow the instructions in the SmartUpdate.



**Note** - A License File can contain multiple licenses.

## Adding a license manually

Step	Instructions
1	Generate a license in the <a href="#">User Center</a> .   <b>Notes:</b> <ul style="list-style-type: none"> <li>■ User Center sends you an e-mail with the license information.</li> <li>■ You can also click the <b>License Information</b> tab to see and copy this information.</li> </ul>
2	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
3	Click the <b>Licenses &amp; Contracts</b> tab.
4	Click the <b>Licenses &amp; Contracts</b> menu at the top > <b>Add License &gt; Manually</b> .
5	In the <b>Add License</b> window you can: <ul style="list-style-type: none"> <li>■ Copy the applicable string from the User Center e-mail and click <b>Paste License</b>.</li> <li>■ Paste the applicable information you copied from the User Center.</li> </ul>  <b>Note</b> - If you leave the <b>Name</b> field empty, the license is assigned a name in the format <SKU>@<Time Date>.
6	Click <b>OK</b> .

# Deleting a License from the Licenses & Contracts Repository

You can delete an unattached license that is no longer needed:

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click the <b>Licenses &amp; Contracts</b> tab.
3	If you do <b>not</b> see the window <b>License And Contract Repository</b> , then click the <b>Licenses &amp; Contracts</b> menu at the top > click <b>View Repository</b> .
4	Right-click anywhere in the <b>Licenses And Contracts Repository</b> window and select <b>View Unattached Licenses</b> .
5	Right-click the <b>Unattached</b> license that you want to delete, and select <b>Delete License / Contract</b> .
6	Click <b>Yes</b> to confirm.

# Attaching a License to a Security Gateway



**Note** - Before you can attach a license to a Security Gateway or Cluster Member, you must add the license to the **Licenses & Contracts Repository**.

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click the <b>Licenses &amp; Contracts</b> tab.
3	Click the <b>Licenses &amp; Contracts</b> menu at the top > click <b>Attach</b> .
4	In the <b>Attach Licenses</b> window, select the applicable Security Gateway or Cluster Member.
5	Click <b>Next</b> .
6	Select the applicable license.
7	Click <b>Finish</b> .
8	Check the <b>Operation Status</b> window.
9	Connect to the command line on the applicable Security Gateway or Cluster Member.
10	Run the "cplic print" command to make sure the license is attached.

# Detaching a License from a Security Gateway

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click the <b>Licenses &amp; Contracts</b> tab.
3	Click the <b>Licenses &amp; Contracts</b> menu at the top > click <b>Detach</b> .
4	In the <b>Detach Licenses</b> window, select the applicable Security Gateway or Cluster Member.
5	Click <b>Next</b> .
6	Select the applicable license.
7	Click <b>Finish</b> .
8	Check the <b>Operation Status</b> window.
9	Connect to the command line on the applicable Security Gateway or Cluster Member.
10	Run the "cplic print" command to make sure the license is detached.

# Getting Licenses from Security Gateways

You can add information from your managed Security Gateways about the licenses you installed locally.

This updates the **Licenses & Contracts Repository** with all local licenses across the installation.

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click the <b>Licenses &amp; Contracts</b> tab.
3	Click the <b>Licenses &amp; Contracts</b> menu at the top > click <b>Get all Licenses</b> .
4	Check the <b>Operation Status</b> window.

# Exporting a License to a File

You can export a license to a file and import it later to the **Licenses & Contracts Repository**. This can be useful for administrative or support purposes.

## Exporting licenses one by one

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate" on page 802.</a>
2	Click <b>Licenses &amp; Contracts</b> tab.
3	If you do <b>not</b> see the window <b>License And Contract Repository</b> , then click the <b>Licenses &amp; Contracts</b> menu at the top > click <b>View Repository</b> .
4	Right-click anywhere in the <b>Licenses And Contracts Repository</b> window and select <b>View all Licenses &amp; Contracts</b> .
5	Right-click the license that you want to export, and select <b>Export License to File</b> .
6	Select the location, enter the applicable file name and click <b>Save</b> .



**Note** - If the license file with such name already exists, the new licenses are added to the existing file.

## Exporting multiple licenses at once

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate" on page 802.</a>
2	Click the <b>Licenses &amp; Contracts</b> tab.
3	If you do <b>not</b> see the window <b>License And Contract Repository</b> , then click the <b>Licenses &amp; Contracts</b> menu at the top> <b>View Repository</b> .
4	Right-click anywhere in the <b>Licenses And Contracts Repository</b> window and select <b>View all Licenses &amp; Contracts</b> .
5	Press and hold the <b>CTRL</b> key.
6	Left-click each license that you want to export.
7	Release the <b>CTRL</b> key.
8	Right-click on one of the selected licenses and select <b>Export License to File</b> .
9	Select the location, enter the applicable file name and click <b>Save</b> .



**Note** - If the license file with such name already exists, the new licenses are added to the existing file.

# Checking for Expired Licenses

If a license expires, the applicable products and features stop working on the Check Point computer, to which the license is attached.



**Best Practice** - We recommend to be aware of the pending expiration dates of all licenses.

## Checking for expired licenses

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click the <b>Licenses &amp; Contracts</b> tab.
3	Click the <b>Licenses &amp; Contracts</b> menu at the top > click <b>Show Expired</b> .
4	In the <b>License/Contract Expiration</b> window, the expired licenses appear in the <b>Expired License and Contracts</b> section.
5	To delete an expired license, select it and click <b>Delete</b> .

## Checking for licenses nearing their dates of expiration

Step	Instructions
1	Open the <b>SmartUpdate</b> . See " <a href="#">Accessing SmartUpdate</a> " on page 802.
2	Click the <b>Licenses &amp; Contracts</b> tab.
3	Click the <b>Licenses &amp; Contracts</b> menu at the top > click <b>Show Expired</b> .
4	In the <b>License/Contract Expiration</b> window, set the applicable number of days in the field <b>Search for licenses/contracts expiring within the next X days</b> .
5	Click <b>Apply</b> to run the search.

# Check Point Cloud Services

## Automatic Downloads

Check Point products connect to Check Point cloud services to download and upload information.

You can enable or disable **Automatic Downloads** in the Gaia First Time Configuration Wizard, on the **Products** page.

We recommend that you enable Automatic Downloads, so that you can use these features:

- *Blade Contracts* are annual licenses for Software Blades and product features. If there is no valid Blade contract, the applicable blades and related features will work, but with some limitations.
- *CPUSE* lets you manage upgrades and installations on Gaia OS. See [sk92449](#).
- *Data updates and Cloud Services* are necessary for the full functionality of these Software Blades and features:
  - Application & URL Filtering
  - Threat Prevention (Anti-Bot, Anti-Virus, Anti-Spam, IPS, Threat Emulation)
  - HTTPS Inspection
  - URL Filtering database
  - Application Database
  - Compliance
  - SmartEndpoint
  - AppWiki
  - ThreatWiki

The Automatic Downloads feature is applicable to the Security Management Servers, Multi-Domain Servers, Log Servers, and Security Gateways.

If you disabled Automatic Downloads in the Gaia First Time Configuration Wizard, you can enable it again in SmartConsole **Global properties**:

Step	Instructions
1	In the top left corner, click <b>Menu &gt; Global properties &gt; Security Management Access</b> .
2	Select <b>Automatically download Contracts and other important data</b> .
3	Click <b>OK</b> .
4	Close the SmartConsole.
5	Connect with SmartConsole to your Management Server.
6	Install the Access Control Policy.

To learn more, see [sk94508](#).

# Sending Data to Check Point

In the Gaia First Time Configuration Wizard, on the **Summary** page, you can enable or disable data uploads to Check Point. This feature is enabled by default. The CPUSE statistics require this feature.

In R77 and above, this setting activates the Check Point User Center Synchronization Tool. It updates your [User Center](#) account with information from your Security Gateways, mapping your SKUs to your actual deployment.

This setting of a Security Management Server applies to all its managed Security Gateways (running R77 and above).

You can always change this setting in SmartConsole:

Step	Instructions
1	In the top left corner, click <b>Menu &gt; Global properties &gt; Security Management Access</b> .
2	Select or clear <b>Improve product experience by sending data to Check Point</b> .
3	Click <b>OK</b> .
4	Close the SmartConsole.
5	Connect with SmartConsole to your Management Server.
6	Install the Access Control Policy.

To learn more, see [sk94509](#).



**Note** - In some cases, the download process sends a minimal amount of required data about your Check Point installation to the Check Point User Center.