



QUANTUM

15 August 2024

INSTALLATION AND UPGRADE GUIDE

R81.20



Check Point Copyright Notice

© 2022 - 2024 Check Point Software Technologies Ltd.

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

RESTRICTED RIGHTS LEGEND:

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

TRADEMARKS:

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

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

Important Information



Latest Software

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



Certifications

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



Check Point R81.20

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



Latest Version of this Document in English

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



Feedback

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

Revision History

Date	Description
15 August 2024	Updated: <ul style="list-style-type: none"> ▪ "Multi-Version Cluster Limitations" on page 427
26 September 2023	Updated: <ul style="list-style-type: none"> ▪ Renamed the cluster upgrade method "Minimal Effort" to "Minimum Effort" ▪ "Minimum Effort Upgrade of a Security Gateway Cluster" on page 473 - Added the missing step to establish SIC with Cluster Members after Clean Install ▪ "Minimum Effort Upgrade of a VSX Cluster" on page 479 - Added the missing step to establish SIC with Cluster Members after Clean Install ▪ Renamed the cluster upgrade method "Zero Downtime" to "Minimum Downtime" to show better the nature of this upgrade method Note - Multi-Version Cluster (MVC) Upgrade is the Zero Downtime Upgrade. ▪ "Minimum Downtime Upgrade of a Security Gateway Cluster" on page 488 - Added the missing steps to establish SIC with Cluster Members after Clean Install ▪ "Minimum Downtime Upgrade of a VSX Cluster" on page 501 - Added the missing steps to establish SIC with Cluster Members after Clean Instal
25 September 2023	Updated: <ul style="list-style-type: none"> ▪ "Installing a CloudGuard Controller" on page 103 - Removed the note about the Known Limitation VSECPC-1341 - it was resolved in R81.20 ▪ "Multi-Version Cluster Upgrade Procedure - Gateway Mode" on page 430 ▪ "Minimum Downtime Upgrade of a Security Gateway Cluster" on page 488 - Updated the notes about changing the CCP mode to Broadcast ▪ "Minimum Downtime Upgrade of a VSX Cluster" on page 501 - Updated the notes about changing the CCP mode to Broadcast
21 February 2023	In the upgrade procedures for Management High Availability Servers, added this note: Make sure the Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794 .

Date	Description
13 February 2023	During an upgrade to R81.20 and higher, the Log Exporter configuration is part of the upgrade.
20 November 2022	First release of this document

Table of Contents

Getting Started	13
Welcome	13
R81.20 Documentation	13
For New Check Point Customers	14
Disk Space	14
Product Deployment Scenarios	14
Backing Up and Restoring	17
The Gaia Operating System	20
Installing the Gaia Operating System on Check Point Appliances	21
Installing the Gaia Operating System on Open Servers	23
Installing a Blink Image to Configure a Check Point Gateway Appliance	25
Changing Disk Partition Sizes During the Installation of Gaia Operating System	26
Running an Unattended USB Installation of Gaia on Check Point Appliances	27
Configuring Gaia for the First Time	28
Running the First Time Configuration Wizard in Gaia Portal	29
Running the First Time Configuration Wizard in CLI Expert mode	47
Configuring the IP Address of the Gaia Management Interface	60
Changing the Disk Partition Sizes on an Installed Gaia	62
Enabling IPv6 on Gaia	63
Installing a Security Management Server	65
Installing One Security Management Server only, or Primary Security Management Server in Management High Availability	66
Installing a Secondary Security Management Server in Management High Availability ..	68
Installing a Dedicated Log Server or SmartEvent Server	71
Deploying a Domain Dedicated Log Server	76
Introduction	76
Procedure for an R81.20 Multi-Domain Environment	76
Procedure for an R77.x Multi-Domain Environment	77

Installing a Multi-Domain Server	82
Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability	83
Installing a Secondary Multi-Domain Server in Management High Availability	85
Installing a Multi-Domain Log Server	88
Installing an Endpoint Server	90
Installing an Endpoint Security Management Server	91
Installing a Secondary Endpoint Security Management Server in Management High Availability	93
Installing an Endpoint Policy Server	96
Connection Port to Services on an Endpoint Security Management Server	98
Disk Space on an Endpoint Security Management Server	102
Installing a CloudGuard Controller	103
Installing a Management Server on Linux	105
Installing SmartConsole	106
Downloading SmartConsole	106
Installing SmartConsole	107
Logging in to SmartConsole	108
Troubleshooting SmartConsole	108
Installing a Security Gateway, VSX Gateway	109
Installing a Security Gateway	110
Installing a VSX Gateway	117
Installing a ClusterXL, VSX Cluster, VRRP Cluster	123
Installing a ClusterXL Cluster	124
Installing a VSX Cluster	151
Installing a VRRP Cluster	160
Full High Availability Cluster on Check Point Appliances	180
Understanding Full High Availability Cluster on Appliances	181
Installing Full High Availability Cluster	182
Recommended Logging Options for a Full High Availability Cluster	187
Installing a Standalone	188

Post-Installation Configuration	192
Installing Software Packages on Gaia	199
Upgrade Options and Prerequisites	202
Prerequisites for Upgrading and Migrating of Management Servers and Log Servers ..	203
Prerequisites for Upgrading and Migrating of Security Gateways and Clusters	210
Prerequisites for Upgrading the Mobile Access Software Blade Configuration	213
Upgrade Methods	215
Contract Verification	220
Upgrade Tools	222
Upgrade of Security Management Servers and Log Servers	224
Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE	225
Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade	232
Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration	243
Upgrading Security Management Servers in Management High Availability from R80.20 and higher	254
Upgrade of Multi-Domain Servers and Multi-Domain Log Servers	260
Upgrading one Multi-Domain Server from R80.20 and higher	261
Upgrading one Multi-Domain Server from R80.20 and higher with CPUSE	262
Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade	269
Upgrading one Multi-Domain Server from R80.20 and higher with Migration	279
Upgrading Multi-Domain Servers in High Availability from R80.20 and higher	289
Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with CPUSE	290
Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade	300
Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration	325
Managing Domain Management Servers During the Upgrade Process	349
Upgrading a Multi-Domain Log Server from R80.20 and higher	350


Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE	351
Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade	356
Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration	363
Upgrade of Endpoint Security Management Servers and Endpoint Policy Servers	370
Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE	371
Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade	377
Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration	388
Upgrading Endpoint Security Management Servers in Management High Availability from R80.20 and higher	399
Upgrade of Security Gateways and Clusters	403
Upgrading a Security Gateway or VSX Gateway	404
Upgrading a Security Gateway with CPUSE	405
Upgrading a VSX Gateway with CPUSE	409
Upgrading ClusterXL, VSX Cluster, or VRRP Cluster	417
Planning a Cluster Upgrade	418
Multi-Version Cluster (MVC) Upgrade	424
Multi-Version Cluster Upgrade Prerequisites	424
Supported Versions in Multi-Version Cluster	425
Multi-Version Cluster Limitations	427
General limitations in Multi-Version Cluster configuration	427
Limitations during failover in Multi-Version Cluster	429
Multi-Version Cluster Upgrade Procedure - Gateway Mode	430
Multi-Version Cluster Upgrade Procedure - VSX Mode	446
Troubleshooting the Multi-Version Cluster	471
Minimum Effort Upgrade	472
Minimum Effort Upgrade of a Security Gateway Cluster	473
Minimum Effort Upgrade of a VSX Cluster	479
Minimum Downtime Upgrade	487

Minimum Downtime Upgrade of a Security Gateway Cluster	488
Minimum Downtime Upgrade of a VSX Cluster	501
Upgrading a Full High Availability Cluster	519
Special Scenarios for Management Servers	520
Backing Up and Restoring a Domain	521
Migrating a Domain Management Server between R81.20 Multi-Domain Servers	524
Migrating Database Between R81.20 Security Management Servers	526
Migrating Database from an R81.20 Security Management Server to an R81.20 Domain Management Server	530
Migrating Database from an R81.20 Domain Management Server to an R81.20 Security Management Server	536
Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server	541
Changing the IP Address of a Domain Management Server or Domain Log Server	548
IPS in Multi-Domain Server Environment	553
Special Scenarios for Security Gateways	554
Deploying a Security Gateway in Monitor Mode	555
Introduction to Monitor Mode	555
Example Topology for Monitor Mode	556
Supported Software Blades in Monitor Mode	556
Limitations in Monitor Mode	558
Configuring a Single Security Gateway in Monitor Mode	559
Configuring a Single VSX Gateway in Monitor Mode	572
Configuring Specific Software Blades for Monitor Mode	584
Configuring the Threat Prevention Software Blades for Monitor Mode	585
Configuring the Application Control and URL Filtering Software Blades for Monitor Mode	587
Configuring the Data Loss Prevention Software Blade for Monitor Mode	588
Configuring the Security Gateway in Monitor Mode Behind a Proxy Server	590
Deploying a Security Gateway or a ClusterXL in Bridge Mode	591
Introduction to Bridge Mode	591
Supported Software Blades in Bridge Mode	591

Limitations in Bridge Mode	594
Configuring a Single Security Gateway in Bridge Mode	595
Configuring a ClusterXL in Bridge Mode	606
Configuring ClusterXL in Bridge Mode - Active / Standby with Two Switches	607
Configuring ClusterXL in Bridge Mode - Active / Active with Two or Four Switches	624
Accept, or Drop Ethernet Frames with Specific Protocols	657
Routing and Bridge Interfaces	659
Managing a Security Gateway through the Bridge Interface	660
IPv6 Neighbor Discovery	663
Managing Ethernet Protocols	663
Configuring Link State Propagation (LSP)	666
Security Before Firewall Activation	670
Boot Security	671
The Initial Policy	677
Troubleshooting: Cannot Complete Reboot	679
Working with Licenses	680
Viewing Licenses in SmartConsole	681
Viewing license information for VSX	682
Monitoring Licenses in SmartConsole	683
Managing Licenses in SmartConsole	688
Managing Licenses in the Gaia Portal	692
Migrating a License to a New IP Address	693
Using Legacy SmartUpdate	696
Accessing SmartUpdate	697
Licenses Stored in the Licenses & Contracts Repository	698
Licensing Terms for SmartUpdate	699
Viewing the Licenses & Contracts Repository	701
Adding New Licenses to the Licenses & Contracts Repository	702
Deleting a License from the Licenses & Contracts Repository	705
Attaching a License to a Security Gateway	706

Detaching a License from a Security Gateway	707
Getting Licenses from Security Gateways	708
Exporting a License to a File	709
Checking for Expired Licenses	711
Check Point Cloud Services	712
Automatic Downloads	712
Sending Data to Check Point	714
Glossary	715

Getting Started

 **Important** - Before you install or upgrade to R81.20:

1. Read the [R81.20 Release Notes](#).
2. Back up the current system. See "[Backing Up and Restoring](#)" on page 17.

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.

R81.20 Documentation

This guide is for administrators responsible for installing R81.20 on appliances and open servers that run the Gaia Operating System.

To learn what is new in R81.20, see the [R81.20 Release Notes](#).

See the [R81.20 Home Page SK](#) for information about the R81.20 release.

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 R81.20, 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.

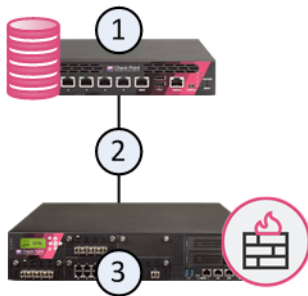
After there is sufficient disk space, install or upgrade the Check Point product.

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).



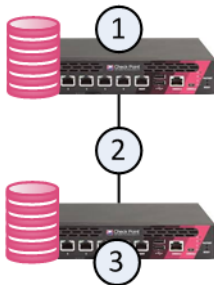
Management High Availability

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.

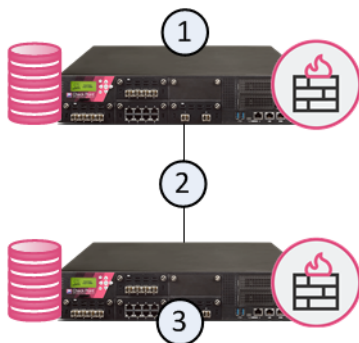
Important - You can deploy and configure a Full High Availability Cluster only on Check Point Appliances that support Standalone configuration. See the [R81.20 Release Notes](#) and *"Installing a Standalone" on page 188*.

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"> ▪ Save a snapshot of your source system. This backs up the entire configuration. ▪ Save a backup of your source system. This file lets you extract the most important configuration easily. ▪ Collect the CPinfo file from your source system (see sk92739). This file lets you see the most important configuration easily with the DiagnosticsView tool (see sk125092).
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"> ▪ Save a second snapshot of your source system. ▪ Save a second backup of your source system. ▪ Collect a second CPinfo file from your source system.
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.

To back up a Security Management Server:

Operating System	Backup Recommendations
Gaia	<ol style="list-style-type: none"> 1. Take the Gaia snapshot. 2. Collect the backup with the "migrate_server export" command. 3. Collect the Log Exporter configuration (see sk127653).
Linux	<ol style="list-style-type: none"> 1. Collect the backup with the "migrate_server export" command. 2. Collect the Log Exporter configuration (see sk127653).

To back up a Multi-Domain Server:

Operating System	Backup Recommendations
Gaia	<ol style="list-style-type: none"> 1. Take the Gaia snapshot. 2. Collect the full backup with the <code>mds_backup</code> command. 3. Collect the Log Exporter configuration (see sk127653).
Linux	<ol style="list-style-type: none"> 1. Collect the full backup with the <code>mds_backup</code> command. 2. Collect the Log Exporter configuration (see sk127653).

To back up a Security Gateway or a Cluster Member:

Operating System	Backup Recommendations
Gaia	Take the Gaia snapshot.

To back up a VSX environment:

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

To back up a Virtual Machine environment:

See the vendor documentation for your virtual platform.

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. *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*
4. *Command Line Interface Reference Guide* - the "migrate_server" command.
5. [sk110173: How to migrate the events database from SmartEvent server R7x to SmartEvent Server R80 and above.](#)
6. [sk100395: How to backup and restore VSX Gateway.](#)
7. [sk127653: How to back up and restore Log Exporter configuration.](#)

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 21](#)
- ["Installing the Gaia Operating System on Open Servers" on page 23](#)
- ["Installing a Blink Image to Configure a Check Point Gateway Appliance" on page 25](#)
- ["Changing Disk Partition Sizes During the Installation of Gaia Operating System" on page 26](#)
- ["Running an Unattended USB Installation of Gaia on Check Point Appliances" on page 27](#)
- ["Configuring Gaia for the First Time" on page 28](#)
- ["Configuring the IP Address of the Gaia Management Interface" on page 60](#)
- ["Changing the Disk Partition Sizes on an Installed Gaia" on page 62](#)
- ["Enabling IPv6 on Gaia" on page 63](#)

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 [R81.20 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: <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre> Loading the system Press any key to see the boot menu [Booting in 5 seconds] </pre> </div>
4	Select Reset to factory defaults and press Enter.
5	Type yes and press Enter.
6	Run the Gaia First Time Configuration Wizard. See " Configuring Gaia for the First Time " on page 28.

Clean install with a Bootable USB device

Step	Instructions
1	Download the Gaia Operating System Clean Install ISO file from the R81.20 Home Page SK.
2	See sk65205 to create a bootable USB device.  Important - Always use the latest available build of the ISomorphic Tool. If you use an outdated build, the installation can fail.
3	Run the Gaia First Time Configuration Wizard. See " Configuring Gaia for the First Time " on page 28.

Clean install with the CPUSE

This option is available if Gaia is already installed.

See "[Installing Software Packages on Gaia](#)" on page 199 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 R81.20 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 "Configuring Gaia for the First Time" on page 28 .

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 R81.20 Home Page SK.
2	See sk65205 to create a bootable USB device.  Important - Always use the latest available build of the ISOMorphic Tool. If you use an outdated build, the installation can fail.
3	Run the Gaia First Time Configuration Wizard. See <i>"Configuring Gaia for the First Time" on page 28</i> .

Clean Install with the CPUSE

This option is available if Gaia is already installed.


See *"Installing Software Packages on Gaia" on page 199* 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	Prepares the USB with these pre-configured settings for a specified network interface: <ul style="list-style-type: none"> ▪ IP address ▪ Network mask ▪ Default Gateway
2	Sends the USB drive to an administrator, who inserts the drive into the appliance and reboots it. The tool installs the Check Point Gaia OS and configures the appliance with the predefined settings. The LCD indicates a successful installation and interfaces blink in round-robin fashion.
3	The first administrator then: <ul style="list-style-type: none"> ▪ Connects to the Gaia Portal and runs the First Time Configuration Wizard, or ▪ Opens a command line to the appliance for further operating system level configuration

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	<p>Connect a computer to the Gaia computer.</p> <p>On Scalable Platforms, connect a computer to the Gaia Management Interface of the Security Group.</p> <p>You must connect to the interface you configured during the Gaia installation (for example, eth0).</p>
2	<p>On your connected computer, configure a static IPv4 address in the same subnet as the IPv4 address you configured during the Gaia installation.</p>
3	<p>On your connected computer, in a web browser, connect to the IPv4 address you configured during the Gaia installation:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>https://<IP address of Gaia Management Interface></pre> </div>
4	<p>Enter the default username and password: <code>admin</code> and <code>admin</code>.</p>
5	<p>Click Login.</p> <p>The Check Point First Time Configuration Wizard opens.</p>
6	<p>Follow the instructions on the First Time Configuration Wizard windows.</p> <p>See the applicable chapters below for installing specific Check Point products.</p>

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



Note - Different windows and fields appear for different products and hardware.

"Deployment Options" window

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

Section	Options	Description
Setup	Continue with R81.20 configuration	Use this option to configure the installed Gaia and Check Point products.
Installation	Install from Check Point Cloud Install from USB device	Use these options to install a Gaia version.
Recovery	Import existing snapshot	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 chooses and installs 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](#).

Scalable Platforms (Maestro and Chassis) do **not** support this feature

"Authentication Details" window

In this window, you configure the main passwords for the Gaia OS.



Section	Description
Change the default administrator password	Configures the password for the Expert mode.
Change the default password for Gaia maintenance mode	Configures the password for the Maintenance Mode (GRUB). This GRUB password protects the GRUB menu and GRUB terminal. Gaia asks for this password when you boot into the Maintenance Mode and when you revert Gaia snapshots.

-  **Note** - You can change each password after you complete the Gaia First Time Configuration Wizard. See [System Passwords](#).
-  **Best Practice** - For security reasons, we recommend to configure a different passwords for the Expert mode and for the Maintenance Mode.

"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
Interface	By default, First Time Configuration Wizard selects the interface you configured during the Gaia installation (for example, eth0).  Note - 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.
Configure IPv4	Select how the Gaia Management Interface gets its IPv4 address: <ul style="list-style-type: none"> ▪ Manually - You configure the IPv4 settings in the next fields. ▪ Off - None.
IPv4 address	Enter the applicable IPv4 address.
Subnet mask	Enter the applicable IPv4 subnet mask.
Default Gateway	Enter the IPv4 address of the applicable default gateway.
Configure IPv6	Select how the Gaia Management Interface gets its IPv6 address: <ul style="list-style-type: none"> ▪ Manually - You configure the IPv6 settings in the next fields. ▪ Off - None.
IPv6 Address	Enter the applicable IPv6 address.  Important - R81.20 does not support IPv6 Address on the Gaia Management Interface (Known Limitation PMTR-47313).
Mask Length	Enter the applicable IPv6 mask length.
Default Gateway	Enter the IPv6 address of the applicable default gateway.

"Internet Connection" window

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

Field	Description
Interface	Select the applicable interface.
Configure IPv4	Select how the applicable interface gets its IPv4 address: <ul style="list-style-type: none"> ▪ Manually - You configure the IPv4 settings in the next fields. ▪ Off - None.
IPv4 address	Enter the applicable IPv4 address.
Subnet mask	Enter the applicable IPv4 subnet mask.
Default Gateway	Enter the IPv4 address of the applicable default gateway.
Configure IPv6	Optional: Select how the applicable interface gets its IPv6 address: <ul style="list-style-type: none"> ▪ Manually - You configure the IPv6 settings in the next fields. ▪ Off - None.
IPv6 Address	Enter the applicable IPv6 address.
Mask Length	Enter the applicable IPv6 mask length.
Default Gateway	Enter the IPv6 address of the applicable default gateway.

"Device Information" window

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

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



"Date and Time Settings" window

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

Field	Description
Set time manually	Select this option to configure the date and time settings manually.
Date	Select the correct date.
Time	Select the correct time.
Time Zone	Select the correct time zone.
Use Network Time Protocol (NTP)	Select this option to configure the date and time settings automatically with NTP.
Primary NTP server	Enter the applicable IPv4 address or resolvable hostname of the primary NTP server.
Version	Select the version of the NTP for the primary NTP server.
Secondary NTP server	Optional: Enter the applicable IPv4 address or resolvable hostname of the secondary NTP server.
Version	Select the version of the NTP for the secondary NTP server.
Time Zone	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
Security Gateway and/or Security Management	Select this option to install: <ul style="list-style-type: none"> ▪ A Single Security Gateway. ▪  Important - Scalable Platforms (Maestro and Chassis) support only this option. ▪ A Cluster Member. ▪ A Security Management Server, including Management High Availability. ▪ An Endpoint Security Management Server. ▪ An Endpoint Policy Server. ▪ CloudGuard Controller. ▪ A dedicated single Log Server. ▪ A dedicated single SmartEvent Server. ▪ A Standalone.
Multi-Domain Server	Select this option to install: <ul style="list-style-type: none"> ▪ A Multi-Domain Server, including Management High Availability. ▪ A dedicated single Multi-Domain Log Server. <p> Important - Scalable Platforms (Maestro and Chassis) do not support this feature</p>


"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
Security Gateway	<p>Select this option to install:</p> <ul style="list-style-type: none"> A single Security Gateway. <ul style="list-style-type: none">  Important - Scalable Platforms (Maestro and Chassis) support only this option. A Cluster Member. A Standalone.
Security Management	<p>Select this option to install:</p> <ul style="list-style-type: none"> A Security Management Server, including Management High Availability. An Endpoint Security Management Server. An Endpoint Policy Server. A CloudGuard Controller. A dedicated single Log Server. A dedicated single SmartEvent Server. A Standalone. <p> Important - Scalable Platforms (Maestro and Chassis) do not support this feature</p>
Unit is a part of a cluster	<p>This option is available only if you selected Security Gateway.</p> <p>Select this option to install a cluster of dedicated Security Gateways, or a Full High Availability Cluster.</p> <p>Select the cluster type:</p> <ul style="list-style-type: none"> ClusterXL - For a cluster of dedicated Security Gateways, or a Full High Availability Cluster. VRRP Cluster - For a VRRP Cluster on Gaia. <p> Important - Scalable Platforms (Maestro and Chassis) do not support this feature</p>

Field	Description
Define Security Management as	<p>Select Primary to install:</p> <ul style="list-style-type: none"> • A Security Management Server. • An Endpoint Security Management Server. • An Endpoint Policy Server. • A CloudGuard Controller. <p>Select Secondary to install:</p> <ul style="list-style-type: none"> • A Secondary Management Server in Management High Availability. <p>Select Log Server / SmartEvent only to install:</p> <ul style="list-style-type: none"> • A dedicated single Log Server. • A dedicated single SmartEvent Server. <p> Important - Scalable Platforms (Maestro and Chassis) do not support this feature</p>

 **Notes** - In this window, you can select to install this Scalable Chassis 60000 / 40000 as a VSX Gateway.

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


Field	Description
Primary Multi-Domain Server	Select this option to install a Primary Multi-Domain Server in Management High Availability.
Secondary Multi-Domain Server	Select this option to install a Secondary Multi-Domain Server in Management High Availability.
Multi-Domain Log Server	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

This window appears if in the **Products** window, you selected only the **Security Gateway** option.

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

Field	Description
Yes	Select this option, if this Security Gateway gets its IP address dynamically (DAIP gateway).  Important - Scalable Platforms (Maestro and Chassis) do not support this feature (Known Limitation MBS-3246).
No	Select this option, if you wish to configure this Security Gateway with a static IP address.

"Secure Communication to Management Server" window

This window appears only if:

- In the **Installation Type** window, you selected the **Security Gateway and/or Security Management** option and in the **Products** window, you selected only the **Security Gateway** option (and optionally, **Unit is a part of a cluster** option)
- In the **Installation Type** window, you selected the **Multi-Domain Server** option and the **Secondary Multi-Domain Server** or the **Multi-Domain Log Server** option.

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
Activation Key	Enter one-time activation key (between 4 and 127 characters long).
Confirm Activation Key	Enter the same one-time activation key again.
Connect to your Management as a Service	This option is available only if in the Products window you selected the Security Gateway option. Select this option if you wish to manage this Security Gateway from the Quantum Smart-1 Cloud service in Infinity Portal.
Authentication token	Enter the token you generated in the Quantum Smart-1 Cloud service. See the Quantum Smart-1 Cloud Administration Guide .

"Security Management Administrator" window

This window appears only if in the **Installation Type** window, you selected the **Security Gateway and/or Security Management** option and in the **Products** window, you selected only the **Security Management** option (and optionally, other options).

In this window, you configure the main Security Management Administrator to log in to SmartConsole.

Field	Description
Use Gaia administrator: admin	Configures the username admin .
Define a new administrator	Configures the user-defined username.

"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
Any IP Address	Select this option to allow all computers to connect.
This machine	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.
Network	Select this option to allow an entire IPv4 subnet of computers to connect. Enter the applicable subnet IPv4 address and subnet mask.
Range of IPv4 addresses	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

This window appears only if in the **Installation Type** window, you selected the **Multi-Domain Server** option.

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

Field	Description
Select leading interface	Select the applicable interface.

"Multi-Domain Server GUI Clients" window

This window appears only if in the **Installation Type** window, you selected the **Multi-Domain Server** option and the **Primary Multi-Domain Server** option.

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

Field	Description
Any host	Select this option to allow all computers to connect.
IP address	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 links at the bottom of this window:

- **End-user License Agreement and Privacy Policy**
- **Update and Data Sharing Settings**

For information about these settings, see [sk175504](#).

Field	Description
Automatically download and install Software Blade Contracts, security updates and other important data (highly recommended)	Controls the download of "Security" data from online Check Point servers: <ul style="list-style-type: none"> • Allows to update the installed Check Point products that are defined as "Security". For example, CPUSE Deployment Agent, Threat Emulation Engine. • Allows to download data that is defined as "Security". For example, signatures for the IPS Software Blade.
Automatically download software updates and new features (highly recommended)	Controls the download of "Non-Security" data from online Check Point servers: <ul style="list-style-type: none"> • Allows to update the installed Check Point products that are defined as "Non-Security". For example, updates for the CPinfo tool. • Allows to download data that is defined as "Non-Security".

Field	Description
<p>Help Check Point improve the product by sending anonymous information</p>	<p>Controls the upload of anonymous data to online Check Point servers:</p> <ul style="list-style-type: none"> • Allows to upload anonymous logs. For example, the upload of logs from the CPUSE tool. • Allows to upload anonymous diagnostics information. For example, the upload of data from the CPinfo and CPUSE tools. <p>Check Point uses this data internally for bug analysis and to improve the products. All data is subject to the European privacy policy (GDPR).</p>
<p>I approve sharing core dump files and other relevant crash data which might contain personal information</p>	<p>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. See the R81.20 Gaia Administration Guide.</p> <p> Warning - Because core dump files contain a snapshot of the memory, they can contain personal and sensitive information.</p>

 **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]#
```

- From a Scalable Platform Security Group:

```
[Expert@HostName-ch0x-0x:0]# g_cat /var/log/ftw_
install.log | egrep --color "installation
succeeded|FTW: Complete"
Dec 06, 19 19:19:51 FTW: Complete
[Expert@HostName-ch0x-0x: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.

 **Important** - On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

Syntax

Viewing the configurable parameters

Form	Command
Short form	<code>config_system -l</code>
Long form	<code>config_system --list-params</code>

Running the First Time Configuration Wizard from a specified configuration file

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

Running the First Time Configuration Wizard from a specified configuration string

Form	Command
Short form	<code>config_system -s <String></code>
Long form	<code>config_system --config-string <String></code>

Creating a First Time Configuration Wizard configuration file template in a specified path

Form	Command
Short form	<code>config_system -t <Path></code>
Long form	<code>config_system --create-template <Path></code>

Making sure the First Time Configuration Wizard configuration file is valid

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

Procedure**Running 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 <String of Parameters and Values></pre> <p>A configuration string must consist of <i>parameter=value</i> pairs, separated by the ampersand (&). You must enclose the whole string between quotation marks. For example:</p> <pre>"hostname=myhost&domainname=somedomain.com&timezone='America/Indiana/Indianapolis'&ftw_sic_key=aaaa&install_security_gw=true&gateway_daip=false&install_ppak=true&gateway_cluster_member=true&install_security_managment=false"</pre> <p>For more information on valid parameters and values, run the "<code>config_system --list-params</code>" command.</p>
2	Reboot the system.

Creating a configuration file

Step	Instructions
1	<p>Run this command in the Expert mode:</p> <pre>config_system -t <File Name></pre>

Step	Instructions
2	Open the file you created in a text editor.
3	Edit all parameter values as necessary.
4	Save the updated configuration file.

Making sure the First Time Configuration Wizard configuration file is valid

Run this command in Expert mode:

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

Running the First Time Configuration Wizard from a configuration file

Step	Instructions
1	Run this command in Expert mode: <pre>config_system -f <File Name></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.

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 --list-params`" command to see the available parameters.

Table: The 'config_system' parameters


Parameter	Supports Scalable Platforms?	Description	Valid values
admin_hash	—	Configures the administrator's password.	A string of alphanumeric characters, enclosed between single quotation marks.
default_gw_v4	—	Specifies IPv4 address of the default gateway.	Single IPv4 address.
default_gw_v6	—	Specifies IPv6 address of the default gateway.	Single IPv6 address.
domainname	—	Configures the domain name (optional).	Fully qualified domain name. Example: somedomain.com
download_info	✓	<p>If its value is set to "true":</p> <ul style="list-style-type: none"> ▪ Downloads and installs Check Point Software Blade contracts. ▪ Downloads and installs Check Point security updates. ▪ Downloads other important information. <p>For more information, see sk94508 and sk175504.</p> <p> Best Practice - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> ▪ true (default) ▪ false

Table: The 'config_system' parameters (continued)



Parameter	Supports Scalable Platforms?	Description	Valid values
download_from_checkpoint_non_security	✓	<p>If its value is set to "true":</p> <ul style="list-style-type: none"> ▪ Downloads Check Point software updates. ▪ Downloads new Check Point features. <p>For more information, see sk94508 and sk175504.</p> <p> Best Practice - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> ▪ true (default) ▪ false
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).
gateway_cluster_member	—	Configures the Security Gateway as member of ClusterXL, if its value is set to "true".	<ul style="list-style-type: none"> ▪ true ▪ false
gateway_daip	—	Configures the Security Gateway as Dynamic IP (DAIP) Security Gateway, if its value is set to "true".	<ul style="list-style-type: none"> ▪ true ▪ false (default) <p> Note - Must be set to "false", if ClusterXL or Security Management Server is enabled.</p>
hostname	✓	Configures the name of the local host (optional).	A string of alphanumeric characters.

Table: The 'config_system' parameters (continued)





Parameter	Supports Scalable Platforms?	Description	Valid values
iface	—	Interface name (optional).	Name of the interface exactly as it appears in the device configuration. Examples: eth0, eth1
install_mds_interface	—	Specifies Multi-Domain Server management interface.	Name of the interface exactly as it appears in the device configuration. Examples: eth0, eth1
install_mds_primary	—	Makes the installed Security Management Server the Primary Multi-Domain Server.  Note - The value of the "install_security_managment" parameter must be set to "true".	<ul style="list-style-type: none"> ■ true ■ false  Note - 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.  Note - The value of the "install_security_managment" parameter must be set to "true".	<ul style="list-style-type: none"> ■ true ■ false  Note - Can only be set to "true", if the value of the "install_mds_primary" parameter is set to "false".

Table: The 'config_system' parameters (continued)



Parameter	Supports Scalable Platforms?	Description	Valid values
install_mgmt_primary	—	<p>Makes the installed Security Management Server the Primary one.</p> <p> Notes:</p> <ul style="list-style-type: none"> Can only be set to "true", if the value of the "install_mgmt_secondary" parameter is set to "false". To install a dedicated Log Server, the value of this parameter must be set to "false". 	<ul style="list-style-type: none"> true false
install_mgmt_secondary	—	<p>Makes the installed Security Management Server a Secondary one.</p> <p> Notes:</p> <ul style="list-style-type: none"> Can only be set to "true", if the value of the "install_mgmt_primary" parameter is set to "false". To install a dedicated Log Server, the value of this parameter must be set to "false". 	<ul style="list-style-type: none"> true false

Table: The 'config_system' parameters (continued)

Parameter	Supports Scalable Platforms?	Description	Valid values
install_mlm	—	Installs Multi-Domain Log Server, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
install_security_gw	—	Installs Security Gateway, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
install_security_managment	—	Installs a Security Management Server or a dedicated Log Server, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
install_security_vsx	✓	Installs VSX Gateway, if its value is set to "true".	<ul style="list-style-type: none"> ■ true ■ false
ipaddr_v4	—	Configures the IPv4 address of the management interface.	Single IPv4 address.
ipaddr_v6	—	Configures the IPv6 address of the management interface.	Single IPv6 address.
ipstat_v4	—	Turns on static IPv4 configuration, if its value is set to "manually".	<ul style="list-style-type: none"> ■ manually (default) ■ off
ipstat_v6	—	Turns static IPv6 configuration on, if its value is set to "manually".	<ul style="list-style-type: none"> ■ manually ■ off (default)
maas_authentication_key	—	Configures the authentication key for Management as a Service (MaaS). Applies only to Security Gateways.	A string of alphanumeric characters, enclosed between single quotation marks.
masklen_v4	—	Configures the IPv4 mask length for the management interface.	A number from 0 to 32.

Table: The 'config_system' parameters (continued)



Parameter	Supports Scalable Platforms?	Description	Valid values
masklen_v6	—	Configures the IPv6 mask length for the management interface.	A number from 0 to 128.
mgmt_admin_name	—	Configures the management administrator's username.  Note - You must specify this parameter, if the value of the "install_security_managment" parameter is set to "true".	A string of alphanumeric characters.
mgmt_admin_passwd	—	Configures the management administrator's password.  Note - You must specify this parameter, if the value of the "install_security_managment" parameter is set to "true".	A string of alphanumeric characters.

Table: The 'config_system' parameters (continued)


Parameter	Supports Scalable Platforms?	Description	Valid values
mgmt_admin_radio	—	Configures Management Server administrator.  Note - You must specify this parameter, if you install a Management Server.	<ul style="list-style-type: none"> ▪ Set the value to "gaia_admin", if you wish to use the Gaia "admin" account. ▪ Set the value to "new_admin", if you wish to configure a new administrator account.
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
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
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_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

Table: The 'config_system' parameters (continued)

Parameter	Supports Scalable Platforms?	Description	Valid values
mgmt_gui_clients_radio	—	Specifies SmartConsole clients that can connect to the Security Management Server.	<ul style="list-style-type: none"> ■ any ■ range ■ network ■ this
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.
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"> ■ 1 ■ 2 ■ 3 ■ 4
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"> ■ 1 ■ 2 ■ 3 ■ 4
primary	—	Configures the IP address of the primary 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.

Table: The 'config_system' parameters (continued)




Parameter	Supports Scalable Platforms?	Description	Valid values
reboot_if_required	—	Reboots the system after the configuration, if its value is set to "true" (optional).	<ul style="list-style-type: none"> ■ true ■ false
secondary	—	Configures the IP address of the secondary DNS server (optional).	IPv4 address.
sg_cluster_id	✓	For Check Point Support use only.	
tertiary	—	Configures the IP address of the tertiary DNS server (optional).	IPv4 address.
timezone	✓	Configures the Area/Region (optional).	<p>The Area/Region must be enclosed between single quotation marks. Examples: 'America/New_York' 'Asia/Tokyo'</p> <p> Note - 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></p>

Table: The 'config_system' parameters (continued)

Parameter	Supports Scalable Platforms?	Description	Valid values
upload_crash_data	✓	<p>Uploads core dump files that help Check Point resolve stability issues, if its value is set to "true". For more information, see the R81.20 Gaia Administration Guide.</p> <p> Warning - The core dump files may contain personal data.</p>	<ul style="list-style-type: none"> ▪ true ▪ false (default)
upload_info	✓	<p>Uploads data that helps Check Point provide you with optimal services, if its value is set to "true". For more information, see sk94509.</p> <p> Best Practice - We highly recommended you enable this optional parameter.</p>	<ul style="list-style-type: none"> ▪ true ▪ false (default)

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: <code>https://<IP Address of Gaia Management Interface></code>
2	In the left navigation tree, go to Network Management > Network Interfaces .
3	In the Management Interface section, click Set Management Interface .
4	Select the applicable interface.
5	Click OK .
6	In the Interfaces section, select the Management Interface and click Edit .
7	Assign the applicable IP address.
8	Click OK .

Changing the IP address in Gaia Clish

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

For more information:


See the [R81.20 Gaia Administration Guide](#).

Changing the Disk Partition Sizes on an Installed Gaia


See the [R81.20 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: <div style="border: 1px solid black; padding: 5px; width: fit-content; margin-top: 5px;">df -h</div>

 **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: <div style="border: 1px solid black; padding: 5px; width: fit-content; margin-top: 5px;">https://<IP address of Gaia Management Interface></div> If you changed the default port of Gaia Portal from 443, then you must also enter it (https://<IP address>:<Port>).
2	In the left navigation tree, click Maintenance > Snapshot Management .  Note - On an Open Server, the available space in the Snapshot Management 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

 **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <pre>https://<IP address of Gaia Management Interface></pre> If you changed the default port of Gaia Portal from 443, then you must also enter it (<code>https://<IP address>:<Port></code>).
2	From the navigation tree, click System Management > System Configuration .
3	In the IPv6 Support section, select On .
4	Click Apply .
5	When prompted, select Yes to reboot.  Important - IPv6 support is not 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	On Scalable Platforms, go to Gaia gClish: Type <code>gclish</code> and press Enter.
4	Enable the IPv6 support: <pre>set ipv6-state on</pre>
5	Save the changes: <pre>save config</pre>

Step	Instructions
6	<p data-bbox="347 237 464 271">Reboot:</p> <div data-bbox="352 277 935 342" style="border: 1px solid #ccc; padding: 2px;"><code data-bbox="373 295 491 322">reboot</code></div> <p data-bbox="352 353 847 427"> Important - IPv6 support is not available until you reboot.</p>

For more information:

See the [R81.20 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 66](#)
- ["Installing a Secondary Security Management Server in Management High Availability" on page 68](#)


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	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28.
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> 1. In the Products section, select Security Management only. 2. In the Clustering section, in the Define Security Management as field, select Primary. ▪ In the Security Management GUI Clients window, configure the applicable allowed computers: <ul style="list-style-type: none"> • Any IP Address - Allows all computers to connect. • This machine - Allows only the single specified computer to connect. • Network - Allows all computers on the specified network to connect. • Range of IPv4 addresses - Allows all computers in the specified range to connect.
4	Install a valid license. See "Working with Licenses" on page 680.

2: Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the Security Management Server object.
4	On the General Properties page, click the Management tab.
5	Enable the applicable Software Blades.  Note - In a Management High Availability environment, the SmartEvent Software Blade is supported only on the Active Management Server (for more information, see sk25164).
6	Click OK .

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 Logs > Storage .
3	Select When disk space is below <number> Mbytes, start deleting old files .
4	Enter the applicable disk space value.
5	Click OK .


For more information:

See the [R81.20 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	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23  Important - You must use the same Gaia installation version as you used for the Primary Security Management Server.
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Management only. b. In the Clustering section, in the Define Security Management as field, select Secondary. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

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 Gateways & Servers .

Step	Instructions
3	<p>Create a new Check Point Host object that represents the Secondary Security Management Server in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click the New (* > More > Check Point Host. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways & Servers > New Check Point Host. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Check Point Host.
4	Click the General Properties page.
5	In the Name field, enter the applicable name.
6	In the IPv4 Address and IPv6 Address fields, enter the applicable IP addresses.
7	<p>In the Platform section:</p> <ul style="list-style-type: none"> ▪ In the Hardware field, select the applicable option ▪ In the Version field, select R81.20 ▪ In the OS field, select Gaia
8	On the General Properties page, click the Management tab.
9	<p>Select Network Policy Management. Make sure the Secondary Server is selected and grayed out.</p> <p> Note - In a Management High Availability environment, the SmartEvent Software Blade is supported only on the Active Management Server (for more information, see sk25164).</p>
10	<p>Establish the Secure Internal Communication (SIC) between the Primary Security Management Server and the Secondary Security Management Server:</p> <ol style="list-style-type: none"> a. In the Secure Internal Communication field, click Communication. b. Enter the same Activation Key you entered during the First Time Configuration Wizard of the Secondary Security Management Server. c. Click Initialize. The Trust state field must show Established. d. Click Close.
11	Click OK .
12	In the SmartConsole top left corner, click Menu > Install database .
13	Select all objects.

Step	Instructions
14	Click Install .
15	Click OK .
16	In the SmartConsole top left corner, click Menu > Management High Availability .
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 Logs > Storage .
3	Select When disk space is below <number> Mbytes, start deleting old files .
4	Enter the applicable disk space value.
5	Click OK .

For more information:

See the [R81.20 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Management only. b. In the Clustering section, in the Define Security Management as field, select Log Server / SmartEvent only. ▪ In the Security Management Administrator window, select one of these options: <ul style="list-style-type: none"> • Use Gaia administrator • Define a new administrator and configure it ▪ In the Security Management GUI Clients window, configure the applicable allowed computers: <ul style="list-style-type: none"> • Any IP Address - Allows all computers to connect. • This machine - Allows only the single specified computer to connect. • Network - Allows all computers on the specified network to connect. • Range of IPv4 addresses - Allows all computers in the specified range to connect. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

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 Gateways & Servers .
3	<p>Create a new Check Point Host object that represents the dedicated Log Server or SmartEvent Server in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click the New (*) > More > Check Point Host. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways & Servers > New Check Point Host. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Check Point Host.
4	Click the General Properties page.
5	In the Name field, enter the applicable name.
6	In the IPv4 Address and IPv6 Address fields, enter the applicable IP addresses.
7	<p>In the Platform section:</p> <ul style="list-style-type: none"> ▪ In the Hardware field, select the applicable option ▪ In the Version field, select R81.20 ▪ In the OS field, select Gaia
8	<p>On the Management tab, select the applicable Software Blades:</p> <ul style="list-style-type: none"> ▪ For the Log Server, select: <ul style="list-style-type: none"> • Logging & Status • Identity Logging, if you work with Identity Awareness Software Blade ▪ For the SmartEvent Server, select: <ul style="list-style-type: none"> • SmartEvent Server • SmartEvent Correlation Unit <p>Note - You can install a dedicated SmartEvent Server and a dedicated SmartEvent Correlation Unit.</p>

Step	Instructions
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">In the Secure Internal Communication field, click Communication.Enter the same Activation Key you entered during the First Time Configuration Wizard of the dedicated Log Server or SmartEvent Server.Click Initialize. The Trust state field must show Established.Click Close.
10	In the left tree, configure the applicable settings.
11	Click OK .
12	In the SmartConsole top left corner, click Menu > Install database .
13	Select all objects.
14	Click Install .
15	Click OK .


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 Logs > Storage .
3	Select When disk space is below <number> Mbytes, start deleting old files .
4	Enter the applicable disk space value.
5	Click OK .

 **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 [R81.20 Security Management Administration Guide](#)
- The [R81.20 Logging and Monitoring Administration Guide](#)
- "[Deploying a Domain Dedicated Log Server](#)" on page 76

Deploying a Domain Dedicated Log Server

Introduction

In a Multi-Domain Security Management environment, the Security Gateways send logs to the Domain Management Server and dedicated Domain Log Servers.

The Multi-Domain Server unifies logs, and they can be stored on the Multi-Domain Server or on a dedicated Multi-Domain Log Server.


Starting in R81, Multi-Domain Server supports a dedicated Log Server (installed on a separate computer) for a Domain.

You can configure a Domain Dedicated Log Server to receive logs only from a specified Domain, and no other Domains can access these logs.

This allows you to locate the dedicated Log Server in a separate network from the Multi-Domain Security Management environment to comply with special regulatory requirements.

Logs reported to the Domain Dedicated Log Server can be viewed from any SmartConsole that has permissions for this Domain.

The Domain Dedicated Log Server communicates directly only with the associated Domain Server. No other Domain can access its log data.

 **Note** - Connecting with SmartConsole to the Domain Dedicated Log Server to see Security Policies is not supported.

Procedure for an R81.20 Multi-Domain Environment

1. Install an R81.20 Multi-Domain Server.
See ["Installing a Multi-Domain Server" on page 82](#).
2. Install a regular dedicated R81.20 Log Server.
See ["Installing a Dedicated Log Server or SmartEvent Server" on page 71](#).
3. Connect with SmartConsole to the specific Domain.
See the [R81.20 Multi-Domain Security Management Administration Guide](#).
4. Add a regular Log Server object for the dedicated R81.20 Log Server you installed in Step 2.

Limitations:

- When a Domainadministrator connects to SmartView on the Multi-Domain Server level or Global SmartEvent Server, the login window shows a picker with the options **MDS**, **Global**, and allowed Domains. The Domainadministrator must select "**Global**" or a specific allowed Domain, according to the assigned permissions.
- An administrator who is connected to a Domain Dedicated Log Server in the assigned Domain cannot see the Domain's data in Views, Reports, and Correlated Events that are based on events from the Global SmartEvent Server.

Requirement post upgrade to R81.20:

For any environment, which uses SmartEvent Server or a Domain Dedicated Log Server, this is a required step to complete post upgrade to R81.20 from any source version:

After you upgrade the SmartEvent Server or Domain Dedicated Log Server, run this command in the Expert mode on each Multi-Domain Security Management Server:

```
$MDS_FWDIR/scripts/cpm.sh -tm -op reset -d all -sd
```

Procedure for an R77.x Multi-Domain Environment

Upgrade with CPUSE

1. Upgrade all servers from R77.x to R80.20 (or R80.30 or R80.40).

This applies to all Multi-Domain Servers, Multi-Domain Log Servers, Domain Dedicated Log Servers, and SmartEvent Servers.

- a. Follow the instructions in the [R80.40 Installation and Upgrade Guide](#).

Important - Stop after the CPUSE Verifier shows the upgrade / installation is allowed.

- For Multi-Domain Servers:

See the chapter "*Upgrade of Multi-Domain Servers and Multi-Domain Log Servers*" > select the applicable section to upgrade "*from R80.10 and lower*" > select the applicable section to upgrade "*with CPUSE*".

- For Log Servers:

See the chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Dedicated Log Server from R80.10 and lower*" > select the applicable section to upgrade "*with CPUSE*".

- For SmartEvent Servers:

See the chapter "*Upgrade of Security Management Servers and Log Servers*" > section "*Upgrading a Dedicated SmartEvent Server from R80.10 and lower*" > select the applicable section to upgrade "*with CPUSE*".

- b. Fix all the errors, except the one specified for Log Servers on a Domain Management Server:

```
Log Servers on the Domain Management Server level are
not yet supported in R80.x
```

- c. On each Multi-Domain Security Management Server, modify the Pre-Upgrade Verifier to treat the upgrade errors as warnings:

- i. Connect to the command line on the Multi-Domain Server.
- ii. Log in to the Expert mode.
- iii. Enter these commands as they appear below (after each command, press the Enter key):

```
cp -v $CPDIR/tmp/.CPprofile.sh{,_BKP}
cat >> $CPDIR/tmp/.CPprofile.sh << EOF
> export PUV_ERRORS_AS_WARNINGS=1
> EOF
```

- d. Restart the CPUSE daemon:

```
DAClient stop ; DAClient start
```

- e. Follow the instructions in the [R80.40 Installation and Upgrade Guide](#) to upgrade all the servers "with CPUSE".

2. Upgrade all Multi-Domain Servers to R81.20.

See "[Upgrade of Multi-Domain Servers and Multi-Domain Log Servers](#)" on page 260 > select the applicable section to upgrade "from R80.20 and higher" > select the applicable section to upgrade "with CPUSE".

3. On each Multi-Domain Security Management Server, run this script in the Expert mode:

```
$MDS_FWDIR/scripts/configureCrldp.sh
```

4. Reboot each Multi-Domain Security Management Server:

```
reboot
```

5. Upgrade all Log Servers and SmartEvent Servers to R81.20.

See "[Upgrade of Security Management Servers and Log Servers](#)" on page 224 > section "Upgrading a Security Management Servers or Log Server from R80.20 and higher" > section "Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade".

Note - To install an R81.20 Log Server or an R81.20 SmartEvent Server, see "[Installing a Dedicated Log Server or SmartEvent Server](#)" on page 71.

6. On each Multi-Domain Security Management Server, run this script in the Expert mode:

```
$MDS_FWDIR/scripts/cpm.sh -tm -op reset -d all -sd
```

7. Reboot all the Domain Dedicated Log Servers and the SmartEvent Servers:

```
reboot
```

Advanced Upgrade

1. Upgrade all servers from R77.x to R80.20 (or R80.30 or R80.40).

This applies to all Multi-Domain Servers, Multi-Domain Log Servers, Domain Dedicated Log Servers, and SmartEvent Servers.

- a. Run the Pre-Upgrade Verifier, as detailed in the [R80.40 Installation and Upgrade Guide](#).

- For Multi-Domain Servers:

See the chapter "[Upgrade of Multi-Domain Servers and Multi-Domain Log Servers](#)" > select the applicable section to upgrade "*from R80.10 and lower*" > select the applicable section to upgrade "*with Advanced Upgrade*".

- For Log Servers:

See the chapter "[Upgrade of Security Management Servers and Log Servers](#)" > section "[Upgrading a Dedicated Log Server from R80.10 and lower](#)" > select the applicable section to upgrade "*with Advanced Upgrade*".

- For SmartEvent Servers:

See the chapter "[Upgrade of Security Management Servers and Log Servers](#)" > section "[Upgrading a Dedicated SmartEvent Server from R80.10 and lower](#)" > select the applicable section to upgrade "*with Advanced Upgrade*".

- b. Fix all the errors, except the one specified for Log Servers on a Domain Management Server:

```
Log Servers on Domain Management Server level are not
yet supported in R80.x
```

- c. In your active shell window, run this command in the Expert mode:

```
export PUV_ERRORS_AS_WARNINGS=1
```

- d. Follow the instructions in the [R80.40 Installation and Upgrade Guide](#) to upgrade all the servers "*with Advanced Upgrade*".

2. Upgrade all Multi-Domain Servers to R81.20.

See "[Upgrade of Multi-Domain Servers and Multi-Domain Log Servers](#)" on page 260 > select the applicable section to upgrade "*from R80.20 and higher*" > select the applicable section to upgrade "*with Advanced Upgrade*".

3. On each Multi-Domain Security Management Server, run this script in the Expert mode:

```
$MDS_FWDIR/scripts/configureCrldp.sh
```

4. Reboot each Multi-Domain Security Management Server:


```
reboot
```

5. Upgrade all Log Servers and SmartEvent Servers to R81.20.

See ["Upgrade of Security Management Servers and Log Servers" on page 224](#) > section ["Upgrading a Security Management Servers or Log Server from R80.20 and higher"](#) > section ["Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade"](#).

i Note - To install an R81.20 Log Server or an R81.20 SmartEvent Server, see ["Installing a Dedicated Log Server or SmartEvent Server" on page 71](#).

6. On each Multi-Domain Security Management Server, run this script in the Expert mode:

```
$MDS_FWDIR/scripts/cpm.sh -tm -op reset -d all -sd
```

7. Reboot all the Domain Dedicated Log Servers and SmartEvent Servers:

```
reboot
```

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 83](#)
- ["Installing a Secondary Multi-Domain Server in Management High Availability" on page 85](#)

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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28.
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Multi-Domain Server. ▪ In the Installation Type window, select Primary Multi-Domain Server. ▪ In the Leading VIP Interfaces Configuration window, select the applicable interface. ▪ In the Multi-Domain Server GUI Clients window, select one of these options: <ul style="list-style-type: none"> • Any host to allow all computers to connect • IP address and enter the IPv4 address of the applicable allowed computer ▪ In the Security Management Administrator window, select one of these options: <ul style="list-style-type: none"> • Use Gaia administrator • Define a new administrator and configure it
4	Install a valid license. See "Working with Licenses" on page 680.

2. Perform initial configuration in SmartConsole

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


For more information:

See the [R81.20 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	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23  Important - You must use the same Gaia installation version as you used for the Primary Multi-Domain Server.
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Multi-Domain Server. ▪ In the Installation Type window, select Secondary Multi-Domain Server. ▪ In the Leading VIP Interfaces Configuration window, select the applicable interface. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Primary Multi-Domain Server - the MDS context.
2	From the left navigation panel, click Multi Domain > Domains .
3	From the top toolbar, click New > Multi-Domain Server .

Step	Instructions
4	Enter the applicable object name.
5	Click the General page.
6	In the Basic Details section: <ul style="list-style-type: none"> a. Enter the applicable IPv4 address. b. Click Connect.
7	Enter the same Activation Key you entered during the setup of First Time Configuration Wizard of the Secondary Multi-Domain Server.
8	Click OK .
7	In the Platform section: <ul style="list-style-type: none"> ■ In the OS field, select Gaia ■ In the Version field, select R81.20 ■ In the Hardware field, select the applicable option
8	Click the Multi-Domain page.
9	Configure the applicable settings.
10	Click the Log Settings > General page.
11	Configure the applicable settings.
12	Click the Log Settings > Advanced Settings page.
13	Configure the applicable settings.
14	Click OK .

 **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 [*R81.20 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Multi-Domain Server. ▪ In the Installation Type window, select Multi-Domain Log Server. ▪ In the Leading VIP Interfaces Configuration window, select the applicable interface. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Primary Multi-Domain Server - the MDS context.
2	From the left navigation panel, click Multi Domain > Domains .
3	From the top toolbar, click New > Multi-Domain Log Server .
4	Enter the applicable object name.
5	Click the General page.

Step	Instructions
6	In the Basic Details section: <ol style="list-style-type: none"> Enter the applicable IPv4 address. Click Connect.
7	Enter the same Activation Key you entered during the First Time Configuration Wizard of the Multi-Domain Log Server.
8	Click OK .
9	In the Platform section: <ul style="list-style-type: none"> ▪ In the OS field, select Gaia ▪ In the Version field, select R81.20 ▪ In the Hardware field, select the applicable option
10	Click the Multi-Domain page.
11	Configure the applicable settings.
12	Click the Log Settings > General page.
13	Configure the applicable settings.
14	Click the Log Settings > Advanced Settings page.
15	Configure the applicable settings.
16	Click OK .

For more information, see:

- The [R81.20 Multi-Domain Security Management Administration Guide](#)
- "[Deploying a Domain Dedicated Log Server](#)" on page 76

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 91](#)
- ["Installing an Endpoint Policy Server" on page 96](#)
- ["Connection Port to Services on an Endpoint Security Management Server" on page 98](#)
- ["Disk Space on an Endpoint Security Management Server" on page 102](#)

Installing an Endpoint Security Management Server

Procedure:

1. Install the Endpoint Security Management Server

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Management only. b. In the Clustering section, in the Define Security Management as field, select Primary. ▪ In the Security Management GUI Clients window, configure the applicable allowed computers: <ul style="list-style-type: none"> • Any IP Address - Allows all computers to connect. • This machine - Allows only the single specified computer to connect. • Network - Allows all computers on the specified network to connect. • Range of IPv4 addresses - Allows all computers in the specified range to connect.
4	Install a valid license. See "Working with Licenses" on page 680 .

2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the Security Management Server object.
4	On the General Properties page, click the Management tab.
5	Select the Endpoint Policy Management blade.
6	Click OK .
7	In the SmartConsole top left corner, click Menu > Install database .
8	Select all objects.
9	Click Install .
10	Click OK .


For more information:

See the [R81.20 Harmony 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	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23 <p> Important - You must use the same Gaia installation version as you used for the Primary Endpoint Security Management Server.</p>
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Management only. b. In the Clustering section, in the Define Security Management as field, select Secondary. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

2. Perform initial configuration in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Primary Endpoint Security Management Server.

Step	Instructions
2	From the left navigation panel, click Gateways & Servers .
3	<p>Create a new Check Point Host object that represents the Secondary Endpoint Security Management Server in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click the New (* > More > Check Point Host. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways & Servers > New Check Point Host. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Check Point Host.
4	Click the General Properties page.
5	In the Name field, enter the applicable name.
6	In the IPv4 Address and IPv6 Address fields, enter the applicable IP addresses.
7	<p>In the Platform section:</p> <ul style="list-style-type: none"> ▪ In the Hardware field, select the applicable option ▪ In the Version field, select R81.20 ▪ In the OS field, select Gaia
8	On the General Properties page, click the Management tab.
9	<p>Select the Network Policy Management and Endpoint Policy Management blades.</p> <p> Note - In a Management High Availability environment, the SmartEvent Software Blade is supported only on the Active Management Server (for more information, see sk25164).</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"> a. In the Secure Internal Communication field, click Communication. b. Enter the same Activation Key you entered during the First Time Configuration Wizard of the Secondary Endpoint Security Management Server. c. Click Initialize. The Trust state field must show Established. d. Click Close.
11	Click OK .
12	In the SmartConsole top left corner, click Menu > Install database .

Step	Instructions
13	Select all objects.
14	Click Install .
15	Click OK .
16	In the SmartConsole top left corner, click Menu > Management High Availability .
17	Make sure the Endpoint Security Management Servers are able to synchronize.

For more information:

See the [R81.20 Harmony 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 91](#).

2. Install the dedicated Endpoint Policy Server

Follow the installation step instructions in ["Installing a Dedicated Log Server or SmartEvent Server" on page 71](#).

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 Gateways & Servers .
3	Create a new Check Point Host object that represents the Endpoint Policy Server in one of these ways: <ul style="list-style-type: none"> ▪ From the top toolbar, click the New (*) > More > Check Point Host. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways & Servers > New Check Point Host. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Check Point Host.
4	Click the General Properties page.
5	In the Name field, enter the applicable name.
6	In the IPv4 Address and IPv6 Address fields, enter the applicable IP addresses.
7	In the Platform section: <ul style="list-style-type: none"> ▪ In the Hardware field, select the applicable option ▪ In the Version field, select R81.20 ▪ In the OS field, select Gaia

Step	Instructions
8	On the Management tab, select both the Endpoint Policy Management and Logging & Status 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">In the Secure Internal Communication field, click Communication.Enter the same Activation Key you entered during the First Time Configuration Wizard of this dedicated Log Server.Click Initialize. The Trust state field must show Established.Click Close.
10	Click OK .
11	In the SmartConsole top left corner, click Menu > Install database .
12	Select all objects.
13	Click Install .
14	Click OK .

For more information:

See the [R81.20 Harmony Endpoint Security Server Administration Guide](#).

Connection Port to Services on an Endpoint Security Management Server

 **Important:**

SSL connection ports on Security Management Servers R81 and higher

- A Security Management Server listens to SSL traffic for *all* services on the TCP port **443** in these cases:
 - If you performed a clean installation of a Security Management Server R81.20 and enabled the **Endpoint Policy Management** Software Blade.
 - If you upgraded a Security Management Server with disabled **Endpoint Policy Management** Software Blade to R81.20 and enabled this Software Blade after the upgrade.

In these cases, when **Endpoint Security** SSL traffic arrives at the TCP port 443, the Security Management Server automatically redirects it (internally) to the TCP port 4434.

Service	URL and Port
Gaia Portal	<code>https://<IP Address of Gaia Management Interface></code>
SmartView Web Application	<code>https://<IP Address of Management Server>/smartview/</code>
Management API Web Services (see Check Point Management API Reference)	<code>https://<IP Address of Management Server>/web_api/<command></code>

- If you upgraded a Security Management Server with enabled **Endpoint Policy Management** Software Blade to R81.20, then the SSL port configuration *remains* as it was in the previous version, from which you upgraded:

- A Security Management Server listens to Endpoint Security SSL traffic on the TCP port 443
- A Security Management Server listens to SSL traffic for *all other* services on the TCP port 4434:

Service	URL and Port
Gaia Portal	https://<IP Address of Gaia Management Interface>:4434
SmartView Web Application	https://<IP Address of Management Server>:4434/smartview/
Management API Web Services (see Check Point Management API Reference)	https://<IP Address of Management Server>:4434/web_api/<command>

In R81 and higher, an administrator can manually configure different TCP ports for the Gaia Portal (and other services) and Endpoint Security - **443** or **4434**. For the applicable procedures, see the [R81.20 Harmony Endpoint Security Server Administration Guide](#) > Chapter *Endpoint Security Architecture* > Section *Connection Port to Services on an Endpoint Security Management Server*.

SSL connection ports on Security Management Servers R80.40 and lower

- 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://<IP Address of Gaia Management Interface></code>
New	<code>https://<IP Address of Gaia Management Interface>:4434</code>

- **SmartView Web Application**

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

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

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

Procedure:

1. Install the CloudGuard Controller

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28.
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Management only. b. In the Clustering section, in the Define Security Management as field, select Primary. ▪ In the Security Management GUI Clients window, configure the applicable allowed computers: <ul style="list-style-type: none"> • Any IP Address - Allows all computers to connect. • This machine - Allows only the single specified computer to connect. • Network - Allows all computers on the specified network to connect. • Range of IPv4 addresses - Allows all computers in the specified range to connect.
4	Install a valid license. See "Working with Licenses" on page 680.

2. Enable the CloudGuard Controller

Step	Instructions
1	Connect to the command line on the Security Management Server.

Step	Instructions
2	Log in to the Gaia Clish, or Expert mode.
3	Run: <pre>cloudguard on</pre>

3. Enable the Identity Awareness Software Blade

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

For more information, see the:

- [R81.20 CloudGuard Controller Administration Guide](#)
- [R81.20 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 [R81.20 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 R81.20 Home Page SK .
2	Go to the Downloads section.
3	Click the SmartConsole link.
4	Save the SmartConsole installation file.

Downloading the SmartConsole package from the Support Center

Step	Instructions
1	Connect to the Check Point Support Center .
2	Search for: <input type="text" value="R81.20 SmartConsole"/>
3	Click the Downloads tab.
4	Click the applicable link to open the download page.
5	Click the Download 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	<p>With a web browser, connect to Gaia Portal at:</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <code>https://<IP address of Gaia Management Interface></code> </div> <p>If you changed the default port of Gaia Portal from 443, then you must also enter it (<code>https://<IP address>:<Port></code>).</p>
2	On the Overview page, click Download Now!
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 SmartConsole 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 Login .
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 [R81.20 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 110](#)
- ["Installing a VSX Gateway" on page 117](#)

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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, clear Unit is a part of a cluster, type. ▪ In the Dynamically Assigned IP window, select the applicable option. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

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 Gateways & Servers .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> • From the top toolbar, click the New (*) > Gateway. • In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > New Gateway. • In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Gateway.
4	In the Check Point Security Gateway Creation window, click Wizard Mode .
5	<p>On the General Properties page:</p> <ol style="list-style-type: none"> a. In the Gateway name field, enter the applicable name for this Security Gateway object. b. In the Gateway platform field, select the correct hardware type. c. In the Gateway IP address section, select the applicable option: <ul style="list-style-type: none"> • If you selected Static IP address, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection 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, click Cancel and follow the procedure Step 2 of 3: Configure the Security Gateway object in SmartConsole - Classic Mode below. d. Click Next.

Step	Instructions
6	<p>On the Trusted Communication page:</p> <ol style="list-style-type: none"> a. Select the applicable option: <ul style="list-style-type: none"> • If you selected Initiate trusted communication now, enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. • If you selected Skip and initiate trusted communication later, make sure to follow Step 7. b. Click Next.
7	<p>On the End page:</p> <ol style="list-style-type: none"> a. Examine the Configuration Summary. b. Select Edit Gateway properties for further configuration. c. Click Finish. <p>Check Point Gateway properties window opens on the General Properties page.</p>
8	<p>If during the Wizard Mode, you selected Skip and initiate trusted communication later:</p> <ol style="list-style-type: none"> a. The Secure Internal Communication field shows <code>Uninitialized</code>. b. Click Communication. c. In the Platform field: <ul style="list-style-type: none"> • Select Open server / Appliance for all Check Point appliance models 3000 and higher. • Select Open server / Appliance for an Open Server. • Select Small Office Appliance only for Check Point Small Office Appliance models lower than 3000. d. Enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. e. Click Initialize. Make sure the Certificate state field shows <code>Established</code>. f. Click OK.
9	<p>On the General Properties page:</p> <ul style="list-style-type: none"> • On the Network Security tab, enable the applicable Software Blades. • On the Threat Prevention tab, enable the applicable Software Blades.
10	Click OK .

Step	Instructions
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 Gateways & Servers .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> • From the top toolbar, click the New (*) > Gateway. • In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > New Gateway. • In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Gateway.
4	<p>In the Check Point Security Gateway Creation window, click Classic Mode.</p> <p>Check Point Gateway properties window opens on the General Properties page.</p>
5	In the Name field, enter the applicable name for this Security Gateway object.
6	<p>In the IPv4 address and IPv6 address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Security 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> <p>If this Security Gateway receives its IP addresses from a DHCP server, select Dynamic Address.</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"> Near the Secure Internal Communication field, click Communication. In the Platform field: <ul style="list-style-type: none"> Select Open server / Appliance for all Check Point models 3000 and higher. Select Open server / Appliance for an Open Server. Enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. Click Initialize. Click OK. <p>If the Certificate state field does not show <code>Established</code>, perform these steps:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Gateway. Make sure there is a physical connectivity between the Security Gateway and the Management Server (for example, pings can pass). Run: <div data-bbox="624 1048 1458 1115" style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>cpconfig</code></div> Enter the number of this option: <div data-bbox="624 1160 1458 1227" style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>Secure Internal Communication</code></div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
8	<p>In the Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: <ul style="list-style-type: none"> If you install the Security Gateway on a Check Point Appliance, select the correct appliances series. If you install the Security Gateway on an Open Server, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.

Step	Instructions
9	Enable the applicable Software Blades: <ul style="list-style-type: none"> • On the Network Security tab. • On the Threat Prevention tab.
10	Click OK .
11	Publish the SmartConsole session.

3. Configure the applicable Security 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 Security Policies ..
3	Create a new policy and configure the applicable layers: <ol style="list-style-type: none"> At the top, click the + tab (or press CTRL T). On the Manage Policies tab, click Manage policies and layers. In the Manage policies and layers window, create a new policy and configure the applicable layers. Click Close. On the Manage Policies tab, click the new policy you created.
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:

- [R81.20 Security Management Administration Guide](#)
- [R81.20 Threat Prevention Administration Guide](#)
- Applicable *Administration Guides* on the [R81.20 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, clear Unit is a part of a cluster, type. ▪ In the Dynamically Assigned IP window, select the applicable option. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

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 [R81.20 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 [R81.20 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 Gateways & Servers .
3	<p>Create a new VSX Gateway object in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click the New (*) > VSX > Gateway. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > VSX > New Gateway. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Gateway. <p>The VSX Gateway Wizard opens.</p>
4	<p>On the VSX Gateway General Properties (Specify the object's basic settings) page:</p> <ol style="list-style-type: none"> a. In the Enter the VSX Gateway Name field, enter the applicable name for this VSX Gateway object. b. In the Enter the VSX Gateway IPv4 field, enter the same IPv4 address that you configured on the Management Connection page of the VSX Gateway's First Time Configuration Wizard. c. In the Enter the VSX Gateway IPv6 field, enter the same IPv6 address that you configured on the Management Connection page of the VSX Gateway's First Time Configuration Wizard. d. In the Select the VSX Gateway Version field, select R81.20. e. Click Next.
5	<p>On the VSX Gateway General Properties (Secure Internal Communication) page:</p> <ol style="list-style-type: none"> a. In the Activation Key field, enter the same Activation Key you entered during the VSX Gateway's First Time Configuration Wizard. b. In the Confirm Activation Key field, enter the same Activation Key again. c. Click Initialize. d. Click Next.

Step	Instructions
	<p>If the Trust State field does not show Trust established, perform these steps:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Make sure there is a physical connectivity between the VSX Gateway and the Management Server (for example, pings can pass). Run: <div data-bbox="509 521 1460 589" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> Enter the number of this option: <div data-bbox="509 633 1460 701" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, on the VSX Gateway General Properties page, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
6	<p>On the VSX Gateway Interfaces (Physical Interfaces Usage) page:</p> <ol style="list-style-type: none"> Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway. If you plan to connect more than one Virtual System directly to the same physical interface, you must select VLAN Trunk for that physical interface. Click Next.
7	<p>On the Virtual Network Device Configuration (Specify the object's basic settings) page:</p> <ol style="list-style-type: none"> You can select Create a Virtual Network Device and configure the first applicable Virtual Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. Click Next.
8	<p>On the VSX Gateway Management (Specify the management access rules) page:</p> <ol style="list-style-type: none"> Examine the default access rules. Select the applicable default access rules. Configure the applicable source objects, if needed. Click Next. <p> Important - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.</p>

Step	Instructions
9	<p>On the VSX Gateway Creation Finalization page:</p> <ol style="list-style-type: none"> Click Finish and wait for the operation to finish. Click View Report for more information. Click Close.
10	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <pre data-bbox="512 602 1460 667">vsx stat -v</pre>
11	Open the VSX Gateway object.
12	On the General Properties page, click the Network Security tab.
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"> ▪ sk79700: VSX supported features on R75.40VS and above ▪ sk106496: Software Blades updates on VSX R75.40VS and above - FAQ ▪ Applicable <i>Administration Guides</i> on the R81.20 Home Page.
14	<p>Click OK to push the updated VSX Configuration.</p> <p>Click View Report for more information.</p>
15	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <pre data-bbox="512 1458 1460 1523">vsx stat -v</pre>
16	<p>Install the default policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the default policy for this VSX Gateway object. <p>This policy is called:</p> <pre data-bbox="512 1767 1460 1832"><Name of VSX Gateway object>_VSX</pre> <ol style="list-style-type: none"> Click Install.

Step	Instructions
17	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>vsx stat -v</pre> </div>
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"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy for this VSX Gateway object. Click Install.
20	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>vsx stat -v</pre> </div>

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 Domain</i> 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.
5	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>vsx stat -v</pre> </div>

Step	Instructions
6	Configure the applicable Threat Prevention Policies for these Virtual Devices.
7	Install the configured Threat Prevention Policies on these Virtual Devices.
8	Examine the VSX configuration: <ol style="list-style-type: none">Connect to the command line on the VSX Gateway.Log in to the Expert mode.Run:<pre>vsx stat -v</pre>

For more information, see the:

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

Installing a ClusterXL, VSX Cluster, VRRP Cluster

This section provides instructions to install a cluster:

- ["Installing a ClusterXL Cluster" on page 124](#)
- ["Installing a VSX Cluster" on page 151](#)
- ["Installing a VRRP Cluster" on page 160](#)
- ["Full High Availability Cluster on Check Point Appliances" on page 180](#)

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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, select these two options: <ul style="list-style-type: none"> • Unit is a part of a cluster • ClusterXL ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .


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 Gateways & Servers .
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> • From the top toolbar, click New (*) > Cluster > Cluster. • In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. • In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.
4	In the Check Point Security Gateway Cluster Creation window, click Wizard Mode .
5	<p>On the Cluster General Properties page:</p> <ol style="list-style-type: none"> a. In the Cluster Name field, enter the applicable name for this ClusterXL object. b. Configure the main Virtual IP address(es) for this ClusterXL object. <ul style="list-style-type: none"> • In the Cluster IPv4 Address section, enter the main Virtual IPv4 address for this ClusterXL object. • In the Cluster IPv6 Address section, enter the main Virtual IPv6 address for this ClusterXL object. <p> Note - 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> c. In the Choose the Cluster's Solution field, select Check Point ClusterXL and select the cluster mode - either High Availability, or Load Sharing. d. Click Next.

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

Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="624 524 1460 584" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">cpconfig</div> Enter the number of this option: <div data-bbox="624 636 1460 696" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">Secure Internal Communication</div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
7	<p>On the Cluster Topology page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> Examine the IPv4 Network Address at the top of the page. Select the applicable role: <ul style="list-style-type: none"> • For <i>cluster traffic interfaces</i>, select Representing a cluster interface and configure the Cluster Virtual IPv4 address and its Net Mask. <div data-bbox="703 1272 1460 1464" style="margin-left: 20px;"> <p> Note - 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> </div> • For <i>cluster synchronization interfaces</i>, select Cluster Synchronization and select Primary only. Check Point cluster supports only one synchronization network. • For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private use of each member (don't monitor members interfaces). Click Next



Step	Instructions
8	<p>On the Cluster Definition Wizard Complete page:</p> <ol style="list-style-type: none"> Examine the Configuration Summary. Select Edit Cluster's Properties. Click Finish <p>The Gateway Cluster Properties window opens.</p>
9	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> In the Name field, make sure you see the configured applicable name for this ClusterXL object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
10	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
11	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab.

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



Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="624 524 1460 584" style="border: 1px solid black; padding: 2px; margin: 5px 0;">cpconfig</div> Enter the number of this option: <div data-bbox="624 636 1460 696" style="border: 1px solid black; padding: 2px; margin: 5px 0;">Secure Internal Communication</div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
13	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select the applicable mode: <ul style="list-style-type: none"> • High Availability and ClusterXL • Load Sharing and Multicast or Unicast • Active-Active In the Tracking section, select the applicable option. In the Advanced Settings section:

Step	Instructions
	<ul style="list-style-type: none"> • If you selected the High Availability mode, then: <ul style="list-style-type: none"> i. Optional: Select Use State Synchronization. This configures the Cluster Members to synchronize the information about the connections they inspect. <ul style="list-style-type: none"> ★ Best Practice - Enable this setting to prevent connection drops after a cluster failover. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> 📘 Notes: <ul style="list-style-type: none"> ◦ 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 R81.20 ClusterXL Administration Guide. ◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. ◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.

Step	Instructions
	<ul style="list-style-type: none"><li data-bbox="651 241 1437 353">iv. Select the Cluster Member recovery method - which Cluster Member to select as Active during a fallback (return to normal operation after a cluster failover):<ul style="list-style-type: none"><li data-bbox="751 360 1366 394">◦ Maintain current active Cluster Member<ul style="list-style-type: none"><li data-bbox="826 405 1461 477">i. The Cluster Member that is currently in the Active state, remains in this state.<li data-bbox="818 488 1433 600">ii. Other Cluster Members that return to normal operation, remain in the Standby state.<li data-bbox="751 607 1374 640">◦ Switch to higher priority Cluster Member<ul style="list-style-type: none"><li data-bbox="826 651 1437 801">i. The Cluster Member that has the highest priority (appears at the top of the list on the Cluster Members page of the cluster object) becomes the new Active.<li data-bbox="818 813 1445 884">ii. The state of the previously Active Cluster Member changes to Standby.<li data-bbox="818 896 1425 1008">iii. Other Cluster Members that return to normal operation remain in the Standby state.


Step	Instructions
	<ul style="list-style-type: none"> • If you selected the Load Sharing > Multicast mode, then: <ul style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> ◦ 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 R81.20 ClusterXL Administration Guide. ◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. ◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.  Best Practice - Enable and configure this setting to increase the cluster performance. iii. Select the connection sharing method between the Cluster Members:

Step	Instructions
	<ul style="list-style-type: none"> <li data-bbox="746 237 1437 797"> <p>○ IPs, Ports, SPIs 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.</p> <li data-bbox="746 808 1465 1155"> <p>○ IPs, Ports 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.</p> <li data-bbox="746 1167 1465 1850"> <p>○ IPs 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. This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>

Step	Instructions
	<ul style="list-style-type: none"> • If you selected the Load Sharing > Unicast mode, then: <ul style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> ◦ 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 R81.20 ClusterXL Administration Guide. ◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. ◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.  Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.


Step	Instructions
	<p>iv. Select the connection sharing method between the Cluster Members:</p> <ul style="list-style-type: none"> <p>○ IPs, Ports, SPIs</p> <p>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.</p> <p>This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</p> <p>This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>We recommend this method.</p> <p>○ IPs, Ports</p> <p>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.</p> <p>Use this method only if there are problems when distributing IPsec packets between Cluster Members.</p> <p>○ IPs</p> <p>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.</p> <p>This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</p> <p>This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>

Step	Instructions
14	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Select each interface and click Edit. The Network: <Name of Interface> window opens. From the left tree, click the General page. In the General section, in the Network Type field, select the applicable type: <ul style="list-style-type: none"> For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct. For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync. <ul style="list-style-type: none"> i Notes: <ul style="list-style-type: none"> We do not recommend the configuration Cluster+Sync. Check Point cluster supports only these settings: <ul style="list-style-type: none"> One Sync interface. One Cluster+Sync interface. One Sync interface and one Cluster+Sync interface. For Check Point Appliances or Open Servers: <p>The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</p> <ul style="list-style-type: none"> For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private.

Step	Instructions
	<p>d. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</p> <p> Notes:</p> <ul style="list-style-type: none"> • For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. • 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 R81.20 ClusterXL Administration Guide. <p>e. In the Topology section:</p> <ul style="list-style-type: none"> • Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> ◦ Override > Network defined by routes (this is the default). ◦ Override > Specific > select the applicable Network object or Network Group object. • To increase the security, enable the Anti-Spoofing.
15	Click OK .
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 Gateways & Servers .
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> • From the top toolbar, click New (*) > Cluster > Cluster. • In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. • In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.
4	<p>In the Check Point Security Gateway Creation window, click Classic Mode.</p> <p>The Gateway Cluster Properties window opens.</p>
5	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> a. In the Name field, make sure you see the configured applicable name for this ClusterXL object. b. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the 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>
6	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> a. In the Hardware field: <ul style="list-style-type: none"> If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. b. In the Version field, select R81.20. c. In the OS field, select Gaia.

Step	Instructions
7	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab.
8	<p>On the Cluster Members page:</p> <ol style="list-style-type: none"> Click Add > New Cluster Member. The Cluster Member Properties window opens. In the Name field, enter the applicable name for this Cluster Member object. Configure the main physical IP address(es) for this Cluster Member object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.  Note - 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. Click Communication. In the One-time password and Confirm one-time password fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard. Click Initialize. Click Close. Click OK. Repeat Steps a-h to add the next Cluster Member.



Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="624 524 1460 586" style="border: 1px solid black; padding: 2px; margin: 5px 0;">cpconfig</div> Enter the number of this option: <div data-bbox="624 636 1460 698" style="border: 1px solid black; padding: 2px; margin: 5px 0;">Secure Internal Communication</div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
9	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select the applicable mode: <ul style="list-style-type: none"> • High Availability and ClusterXL • Load Sharing and Multicast or Unicast • Active-Active In the Tracking section, select the applicable option. In the Advanced Settings section:

Step	Instructions
	<ul style="list-style-type: none"> • If you selected the High Availability mode, then: <ol style="list-style-type: none"> i. Optional: Select Use State Synchronization. This configures the Cluster Members to synchronize the information about the connections they inspect. <ul style="list-style-type: none"> ★ Best Practice - Enable this setting to prevent connection drops after a cluster failover. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> 📘 Notes: <ul style="list-style-type: none"> ◦ 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 R81.20 ClusterXL Administration Guide. ◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. ◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.

Step	Instructions
	<ul style="list-style-type: none"><li data-bbox="651 241 1437 353">iv. Select the Cluster Member recovery method - which Cluster Member to select as Active during a fallback (return to normal operation after a cluster failover):<ul style="list-style-type: none"><li data-bbox="751 360 1366 394">◦ Maintain current active Cluster Member<ul style="list-style-type: none"><li data-bbox="826 405 1461 477">i. The Cluster Member that is currently in the Active state, remains in this state.<li data-bbox="818 488 1433 600">ii. Other Cluster Members that return to normal operation, remain in the Standby state.<li data-bbox="751 607 1374 640">◦ Switch to higher priority Cluster Member<ul style="list-style-type: none"><li data-bbox="826 651 1437 801">i. The Cluster Member that has the highest priority (appears at the top of the list on the Cluster Members page of the cluster object) becomes the new Active.<li data-bbox="818 813 1445 884">ii. The state of the previously Active Cluster Member changes to Standby.<li data-bbox="818 896 1425 1008">iii. Other Cluster Members that return to normal operation remain in the Standby state.

Step	Instructions
	<ul style="list-style-type: none"> • If you selected the Load Sharing > Multicast mode, then: <ol style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> ◦ 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 R81.20 ClusterXL Administration Guide. ◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. ◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.  Best Practice - Enable and configure this setting to increase the cluster performance. iii. Select the connection sharing method between the Cluster Members:

Step	Instructions
	<ul style="list-style-type: none"> <li data-bbox="746 237 1442 797"> <p>○ IPs, Ports, SPIs 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.</p> <li data-bbox="746 808 1442 1155"> <p>○ IPs, Ports 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.</p> <li data-bbox="746 1167 1442 1850"> <p>○ IPs 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. This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>

Step	Instructions
	<ul style="list-style-type: none"> • If you selected the Load Sharing > Unicast mode, then: <ol style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> ◦ 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 R81.20 ClusterXL Administration Guide. ◦ The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. ◦ The connections that the Cluster Members did not synchronize, do not survive a cluster failover.  Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.

Step	Instructions
	<p>iv. Select the connection sharing method between the Cluster Members:</p> <ul style="list-style-type: none"> <p>○ IPs, Ports, SPIs</p> <p>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.</p> <p>This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</p> <p>This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>We recommend this method.</p> <p>○ IPs, Ports</p> <p>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.</p> <p>Use this method only if there are problems when distributing IPsec packets between Cluster Members.</p> <p>○ IPs</p> <p>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.</p> <p>This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</p> <p>This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>

Step	Instructions
10	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Select each interface and click Edit. The Network: <Name of Interface> window opens. From the left tree, click the General page. In the General section, in the Network Type field, select the applicable type: <ul style="list-style-type: none"> For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct. For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync. <ul style="list-style-type: none"> i Notes: <ul style="list-style-type: none"> We do not recommend the configuration Cluster+Sync. Check Point cluster supports only these settings: <ul style="list-style-type: none"> One Sync interface. One Cluster+Sync interface. One Sync interface and one Cluster+Sync interface. For Check Point Appliances or Open Servers: <p>The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.</p> <ul style="list-style-type: none"> For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private.

Step	Instructions
	<p>d. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</p> <p>i Notes:</p> <ul style="list-style-type: none"> • For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. • 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 R81.20 ClusterXL Administration Guide. <p>e. In the Topology section:</p> <ul style="list-style-type: none"> • Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> ◦ Override > Network defined by routes (this is the default). ◦ Override > Specific > select the applicable Network object or Network Group object. • To increase the security, enable the Anti-Spoofing.
11	Click OK .
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 Security Policies .

Step	Instructions
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> At the top, click the + tab (or press CTRL T). On the Manage Policies tab, click Manage policies and layers. In the Manage policies and layers window, create a new policy and configure the applicable layers. Click Close. On the Manage Policies tab, click the new policy you created.
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"> ■ In Gaia Clish, run: <pre>show cluster state</pre> ■ In the Expert mode, run: <pre>cphaprob state</pre>
3	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show cluster members interfaces all</pre> ■ In the Expert mode, run: <pre>cphaprob -a if</pre>

For more information, see the:

- [R81.20 Security Management Administration Guide](#).
- [R81.20 ClusterXL Administration Guide](#).
- Applicable *Administration Guides* on the [R81.20 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, select these two options: <ul style="list-style-type: none"> • Unit is a part of a cluster • ClusterXL ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .


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 [R81.20 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 [R81.20 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.
2	From the left navigation panel, click Gateways & Servers .
3	<p>Create a new VSX Cluster object in one of these ways:</p> <ul style="list-style-type: none"> ■ From the top toolbar, click the New (*) > VSX > Cluster. ■ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > VSX > New Cluster. ■ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Cluster.
4	<p>On the VSX Cluster General Properties (Specify the object's basic settings) page:</p> <ol style="list-style-type: none"> a. In the Enter the VSX Cluster Name field, enter the applicable name for this VSX Cluster object. b. In the Enter the VSX Cluster IPv4 field, enter the Cluster Virtual IPv4 address that is configured on the Dedicated Management Interfaces (DMI). c. In the Enter the VSX Cluster IPv6 field, enter the Cluster Virtual IPv6 address that is configured on the Dedicated Management Interfaces (DMI). d. In the Select the VSX Cluster Version field, select R81.20. e. In the Select the VSX Cluster Platform field, select the applicable VSX Cluster mode: <ul style="list-style-type: none"> ■ ClusterXL (for High Availability) ■ ClusterXL Virtual System Load Sharing f. Click Next.

Step	Instructions
5	<p>On the VSX Cluster Members (Define the members of this VSX Cluster) page, add the objects for the VSX Cluster Members:</p> <ol style="list-style-type: none"> Click Add. In the Cluster Member Name field, enter the applicable name for this Cluster Member object. In the Cluster Member IPv4 Address field, enter the IPv4 address of the Dedicated Management Interface (DMI). In the Enter the VSX Gateway IPv6 field, enter the applicable IPv6 address. In the Activation Key and Confirm Activation Key fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard. Click Initialize. Click OK. Repeat Steps a-f to add the second VSX Cluster Member, and so on. <p>If the Trust State field does not show Trust established, perform these steps:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Cluster Member. Make sure there is a physical connectivity between the VSX Cluster Member and the Management Server (for example, pings can pass). Run: <div data-bbox="512 1211 1460 1274" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> Enter the number of this option: <div data-bbox="512 1323 1460 1386" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
6	<p>On the VSX Cluster Interfaces (Physical Interfaces Usage) page:</p> <ol style="list-style-type: none"> Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway. If you plan to connect more than one Virtual System directly to the same physical interface, you must select VLAN Trunk for that physical interface. Click Next.

Step	Instructions
7	<p>On the VSX Cluster members (Synchronization Network) page:</p> <ol style="list-style-type: none"> Select the interface that will be used for state synchronization. Configure the IPv4 addresses for the Sync interfaces on each Cluster Member. Click Next.
8	<p>On the Virtual Network Device Configuration (Specify the object's basic settings) page:</p> <ol style="list-style-type: none"> You can select Create a Virtual Network Device and configure the first applicable Virtual Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. Click Next.
9	<p>On the VSX Gateway Management (Specify the management access rules) page:</p> <ol style="list-style-type: none"> Examine the default access rules. Select the applicable default access rules. Configure the applicable source objects, if needed. Click Next. <p> Important - 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 VSX Gateway Creation Finalization page:</p> <ol style="list-style-type: none"> Click Finish and wait for the operation to finish. Click View Report for more information. Click Close.
11	<p>Examine the VSX Cluster configuration:</p> <ol style="list-style-type: none"> Connect to the command line on each VSX Cluster Member. Log in to the Expert mode. Run: <pre style="border: 1px solid black; padding: 5px; width: fit-content;">vsx stat -v</pre>
12	<p>In SmartConsole, open the VSX Cluster object.</p>

Step	Instructions
13	<p>On the General Properties page > the Network Security tab:</p> <ol style="list-style-type: none"> Make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades for the VSX Cluster object itself (context of VS0). <p>Refer to:</p> <ul style="list-style-type: none"> ▪ sk79700: VSX supported features on R75.40VS and above ▪ sk106496: Software Blades updates on VSX R75.40VS and above - FAQ ▪ Applicable <i>Administration Guides</i> on the R81.20 Home Page.
14	<p>Click OK to push the updated VSX Configuration. Click View Report for more information.</p>
15	<p>Install the default policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the default policy for this VSX Cluster object. This policy is called: <div data-bbox="512 965 1460 1025" style="border: 1px solid gray; padding: 2px; margin: 5px 0;"> <p style="margin: 0;"><i><Name of VSX Cluster object>_VSX</i></p> </div> Click Install.

Step	Instructions
16	<p>Examine the VSX configuration and cluster state:</p> <ol style="list-style-type: none"> Connect to the command line on <i>each</i> VSX Cluster Member. Examine the VSX configuration: In the Expert mode, run: <div data-bbox="512 405 1460 468" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>vsx stat -v</pre> </div> <ul style="list-style-type: none">  Important: <ul style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy. Examine the cluster state in one of these ways: <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <div data-bbox="592 728 1460 831" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>set virtual-system 0 show cluster state</pre> </div> ▪ In the Expert mode, run: <div data-bbox="592 882 1460 985" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>vsenv 0 cphaprob state</pre> </div> <ul style="list-style-type: none">  Important: <ul style="list-style-type: none"> ▪ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members. ▪ One VSX Cluster Member must be in the Active state, and all other VSX Cluster Members must be in Standby state. ▪ All Virtual Systems must show the same information about the states of all Virtual Systems. Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <div data-bbox="592 1406 1460 1509" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>set virtual-system 0 show cluster members interfaces all</pre> </div> ▪ In the Expert mode, run: <div data-bbox="592 1561 1460 1664" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>vsenv 0 cphaprob -a if</pre> </div>

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 Domain Management Server</i> 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"> Connect to the command line on <i>each</i> VSX Cluster Member. Examine the VSX configuration: <p>In the Expert mode, run:</p> <pre data-bbox="512 405 1460 468">vsx stat -v</pre> <p>i Important:</p> <ul style="list-style-type: none"> Make sure all the configured Virtual Devices are loaded. Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy. Examine the cluster state in one of these ways: <ul style="list-style-type: none"> In Gaia Clish, run: <pre data-bbox="592 728 1460 831">set virtual-system 0 show cluster state</pre> In the Expert mode, run: <pre data-bbox="592 882 1460 985">vsenv 0 cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> All VSX Cluster Members must show the same information about the states of all VSX Cluster Members. One VSX Cluster Member must be in the Active state, and all other VSX Cluster Members must be in Standby state. All Virtual Systems must show the same information about the states of all Virtual Systems. Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> In Gaia Clish, run: <pre data-bbox="592 1406 1460 1509">set virtual-system 0 show cluster members interfaces all</pre> In the Expert mode, run: <pre data-bbox="592 1561 1460 1664">vsenv 0 cphaprob -a if</pre>

For more information, see the:

- [*R81.20 Security Management Administration Guide.*](#)
- [*R81.20 VSX Administration Guide.*](#)
- [*R81.20 ClusterXL Administration Guide.*](#)
- Applicable *Administration Guides* on the [R81.20 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, select these two options: <ul style="list-style-type: none"> • Unit is a part of a cluster • VRRP Cluster ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .
5	On Gaia, VRRP can be used with ClusterXL <i>enabled</i> or with ClusterXL <i>disabled</i> . See the R81.20 Gaia Administration Guide - 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"> a. When prompted to reboot, click Cancel. b. Connect to the command line. c. Run: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>cpconfig</pre> </div> d. Select Enable cluster membership for this gateway to enable State synchronization. Enter y when prompted. e. Exit from the <code>cpconfig</code> menu.
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 [R81.20 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 Gateways & Servers .
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> • From the top toolbar, click New (*) > Cluster > Cluster. • In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. • In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.
4	In the Check Point Security Gateway Cluster Creation window, click Wizard Mode .
5	<p>On the Cluster General Properties page:</p> <ol style="list-style-type: none"> a. In the Cluster Name field, enter the applicable name for this VRRP Cluster object. b. Configure the main Virtual IP address(es) for this VRRP Cluster object. <ul style="list-style-type: none"> • In the Cluster IPv4 Address section, enter the main Virtual IPv4 address for this VRRP Cluster object. • In the Cluster IPv6 Address section, enter the main Virtual IPv6 address for this VRRP Cluster object. <p> Note - 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> c. In the Choose the Cluster's Solution field, select Gaia VRRP. d. Click Next.


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


Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="624 524 1460 584" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">cpconfig</div> Enter the number of this option: <div data-bbox="624 636 1460 696" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">Secure Internal Communication</div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
7	<p>On the Cluster Topology page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> Examine the IPv4 Network Address at the top of the page. Select the applicable role: <ul style="list-style-type: none"> • For <i>cluster traffic interfaces</i>, select Representing a cluster interface and configure the Cluster Virtual IPv4 address and its Net Mask. <div data-bbox="703 1272 1460 1464" style="margin-left: 20px;"> <p> Note - 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> </div> • For <i>cluster synchronization interfaces</i>, select Cluster Synchronization and select Primary only. Check Point cluster supports only one synchronization network. • For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private use of each member (don't monitor members interfaces). Click Next

Step	Instructions
8	<p>On the Cluster Definition Wizard Complete page:</p> <ol style="list-style-type: none"> Examine the Configuration Summary. Select Edit Cluster's Properties. Click Finish <p>The Gateway Cluster Properties window opens.</p>
9	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> In the Name field, enter the applicable name for this VRRP Cluster object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
10	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
11	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab.

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


Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="624 524 1460 584" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">cpconfig</div> Enter the number of this option: <div data-bbox="624 636 1460 696" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">Secure Internal Communication</div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
13	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select High Availability and VRRP. In the Tracking section, select the applicable option. In the Advanced Settings section: <ul style="list-style-type: none"> • Optional: Select Use State Synchronization • Optional: Select Hide Cluster Members outgoing traffic behind the Cluster IP Address • Optional: Select Forward Cluster incoming traffic to Cluster Members IP Addresses <p>For more information, click the (?) button in the top right corner.</p> <p> Best Practice - We recommend to select all these optional settings.</p>


Step	Instructions
14	<p>On the Network Management page:</p> <ol style="list-style-type: none">Select each interface and click Edit. The Network: <Name of Interface> window opens.From the left tree, click the General page.In the General section, in the Network Type field, select the applicable type:<ul style="list-style-type: none">For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync. <p> Notes:</p> <ul style="list-style-type: none">We do not recommend the configuration Cluster+Sync.Check Point cluster supports only these settings:<ul style="list-style-type: none">One Sync interface.One Cluster+Sync interface.One Sync interface and one Cluster+Sync interface.For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface. <ul style="list-style-type: none">For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private.


Step	Instructions
	<p>d. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</p> <p> Notes:</p> <ul style="list-style-type: none"> • For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. • 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 R81.20 ClusterXL Administration Guide. <p>e. In the Topology section:</p> <ul style="list-style-type: none"> • Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> ◦ Override > Network defined by routes (this is the default). ◦ Override > Specific > select the applicable Network object or Network Group object. • To increase the security, enable the Anti-Spoofing.
15	Click OK .
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 Gateways & Servers .
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> • From the top toolbar, click New (*) > Cluster > Cluster. • In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. • In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.
4	<p>In the Check Point Security Gateway Cluster Creation window, click Classic Mode.</p> <p>The Gateway Cluster Properties window opens.</p>
5	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> a. In the Name field, enter the applicable name for this VRRP Cluster object. b. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the 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>
6	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> a. In the Hardware field: <ul style="list-style-type: none"> If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. b. In the Version field, select R81.20. c. In the OS field, select Gaia.

Step	Instructions
7	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab.
8	<p>On the Cluster Members page:</p> <ol style="list-style-type: none"> Click Add > New Cluster Member. The Cluster Member Properties window opens. In the Name field, enter the applicable name for this VRRP Cluster Member object. Configure the main physical IP address(es) for this VRRP Cluster Member object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.  Note - 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. Click Communication. In the One-time password and Confirm one-time password fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard. Click Initialize. Click Close. Click OK. Repeat Steps a-h to add the second Cluster Member.

Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="624 524 1460 584" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">cpconfig</div> Enter the number of this option: <div data-bbox="624 636 1460 696" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;">Secure Internal Communication</div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
9	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select High Availability and VRRP. In the Tracking section, select the applicable option. In the Advanced Settings section: <ul style="list-style-type: none"> • Optional: Select Use State Synchronization • Optional: Select Hide Cluster Members outgoing traffic behind the Cluster IP Address • Optional: Select Forward Cluster incoming traffic to Cluster Members IP Addresses <p>For more information, click the (?) button in the top right corner.</p> <p> Best Practice - We recommend to select all these optional settings.</p>

Step	Instructions
10	<p>On the Network Management page:</p> <ol style="list-style-type: none">Select each interface and click Edit. The Network: <Name of Interface> window opens.From the left tree, click the General page.In the General section, in the Network Type field, select the applicable type:<ul style="list-style-type: none">For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct.For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync.<ul style="list-style-type: none"> Notes:<ul style="list-style-type: none">We do not recommend the configuration Cluster+Sync.Check Point cluster supports only these settings:<ul style="list-style-type: none">One Sync interface.One Cluster+Sync interface.One Sync interface and one Cluster+Sync interface.For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface.For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private.

Step	Instructions
	<p>d. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member.</p> <p>i Notes:</p> <ul style="list-style-type: none"> For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. 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 R81.20 ClusterXL Administration Guide. <p>e. In the Topology section:</p> <ul style="list-style-type: none"> Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> Override > Network defined by routes (this is the default). Override > Specific > select the applicable Network object or Network Group object. To increase the security, enable the Anti-Spoofing.
11	Click OK .
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 Security Policies .

Step	Instructions																																				
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> At the top, click the + tab (or press CTRL T). On the Manage Policies tab, click Manage policies and layers. In the Manage policies and layers window, create a new policy and configure the applicable layers. Click Close. On the Manage Policies tab, click the new policy you created. 																																				
4	<p>Create the required Access Control rules. 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"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services & Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </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> <p>If the VRRP Cluster Members use dynamic routing protocols (such as OSPF or RIP), create new rules for each multicast destination IP address. Alternatively, you can create a Network object to represent all multicast network IP destinations:</p> <ul style="list-style-type: none"> ▪ Name: <code>MCAST.NET</code> (this is an example name) ▪ IP Address: <code>224.0.0.0</code> ▪ Net mask: <code>240.0.0.0</code> <p>You can use one rule for all multicast protocols you agree to accept, as shown in this example:</p> <table border="1"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services & Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>All multicast protocols</td> <td>VRRP Cluster object</td> <td>VRRP Cluster object <code>MCAST.NET</code></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 On	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 On	1	All multicast protocols	VRRP Cluster object	VRRP Cluster object <code>MCAST.NET</code>	Any	vrrp igmp ospf rip	Accept	None	VRRP Cluster object
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On																													
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 On																													
1	All multicast protocols	VRRP Cluster object	VRRP Cluster object <code>MCAST.NET</code>	Any	vrrp igmp ospf rip	Accept	None	VRRP Cluster object																													
5	Configure additional applicable Access Control rules.																																				

Step	Instructions
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	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show cluster state</pre> ■ In the Expert mode, run: <pre>cphaprob state</pre>
3	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show cluster members interfaces all</pre> ■ In the Expert mode, run: <pre>cphaprob -a if</pre>
4	Examine the VRRP configuration in one of these ways: <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show vrrp</pre> ■ In the Expert mode, run: <pre>clish -c "show vrrp"</pre>

For more information, see the:

- [R81.20 Security Management Administration Guide.](#)
- [R81.20 ClusterXL Administration Guide.](#)
- [R81.20 Gaia Administration Guide.](#)
- Applicable *Administration Guides* on the [R81.20 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.

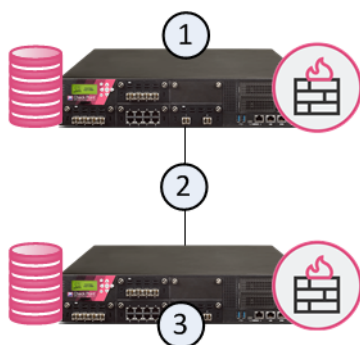
i Important - You can deploy and configure a Full High Availability Cluster only on Check Point Appliances that support Standalone configuration. See the [R81.20 Release Notes](#) and "[Installing a Standalone](#)" on page 188.

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 [R81.20 ClusterXL Administration Guide](#).

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

i 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 71).

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	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select both Security Gateway and Security Management. b. In the Clustering section: <ul style="list-style-type: none"> • Select Unit is a part of a cluster, type and select ClusterXL. • In the Define Security Management as field, select Primary. ▪ In the Security Management Administrator window, select one of these options: <ul style="list-style-type: none"> • Use Gaia administrator • Define a new administrator and configure it ▪ In the Security Management GUI Clients window, configure the applicable allowed computers: <ul style="list-style-type: none"> • Any IP Address - Allows all computers to connect • This machine - Allows only the single specified computer to connect • Network - Allows all computers on the specified network to connect • Range of IPv4 addresses - Allows all computers in the specified range to connect

Step	Instructions
4	Install a valid license. See "Working with Licenses" on page 680 .
5	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"><code>https://<IP address of Gaia Management Interface></code></div> If you changed the default port of Gaia Portal from 443, then you must also enter it (<code>https://<IP address>:<Port></code>).
6	In the left navigation tree, click Network Management > Network Interfaces . Configure all required interfaces with applicable unique IP addresses.

2. Install the second Cluster Member of the Full High Availability Cluster that runs the Secondary Security Management Server

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select both Security Gateway and Security Management. b. In the Clustering section: <ul style="list-style-type: none"> • Select Unit is a part of a cluster, type and select ClusterXL. • In the Define Security Management as field, select Secondary. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).
4	Install a valid license. See "Working with Licenses" on page 680 .

Step	Instructions
5	<p>With a web browser, connect to Gaia Portal at:</p> <pre>https://<IP address of Gaia Management Interface></pre> <p>If you changed the default port of Gaia Portal from 443, then you must also enter it (<code>https://<IP address>:<Port></code>).</p>
6	<p>In the left navigation tree, click Network Management > Network Interfaces.</p> <p>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 R81.20 ClusterXL Administration Guide - 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> <pre>https://<IP address of Gaia Management Interface></pre>
3	<p>In the left navigation tree, click Network Management > Network Interfaces.</p>
4	<p>In the top right corner, click the Configuration button.</p>
5	<p>Make sure the Link Status on the synchronization interfaces is Up.</p>
6	<p>In the top right corner, click the Monitoring button.</p>
7	<p>Click Refresh every several seconds.</p> <p>These counters must increase:</p> <ul style="list-style-type: none"> ▪ Rbytes ▪ Rpackets ▪ Tbytes ▪ Tpackets

4. Install the R81.20 SmartConsole

Follow "[Installing SmartConsole](#)" on page 106.

5. Configure the Full High Availability Cluster object in SmartConsole

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

- [R81.20 Gaia Administration Guide](#)
- [R81.20 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 " Installing a Dedicated Log Server or SmartEvent Server " on page 71.
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 Gateways & Servers .
4	Open the cluster object.
5	From the left navigation tree, click Logs > Additional Logging Configuration .
6	Select Forward log files to Log Server and select the object of the dedicated Log Server.
7	In the Log forwarding schedule field, select or define a Scheduled Event object.
8	Click OK .
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 [R81.20 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 [R81.20 Release Notes](#).

1. Install the Standalone

Step	Instructions
1	Install the Gaia Operating System: <ul style="list-style-type: none"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28.
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select both Security Gateway and Security Management. b. In the Clustering section: <ul style="list-style-type: none"> • Clear Unit is a part of a cluster, type. • In the Define Security Management as field, select Primary. ▪ In the Security Management Administrator window, select one of these options: <ul style="list-style-type: none"> • Use Gaia administrator • Define a new administrator and configure it ▪ In the Security Management GUI Clients window, configure the applicable allowed computers: <ul style="list-style-type: none"> • Any IP Address - Allows all computers to connect • This machine - Allows only the single specified computer to connect • Network - Allows all computers on the specified network to connect • Range of IPv4 addresses - Allows all computers in the specified range to connect

2. Configure the Standalone object in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Standalone.
2	From the left navigation panel, click Gateways & Servers .

Step	Instructions
3	Open the Standalone object. Check Point Gateway properties window opens on the General Properties page.
4	In the Platform section, select the correct options: <ul style="list-style-type: none"> a. In the Hardware field: <ul style="list-style-type: none"> ▪ If you install the Security Gateway on a Check Point Appliance, select the correct appliances series. ▪ If you install the Security Gateway on an Open Server, select Open server. b. Make sure the Version field shows R81.20. c. In the OS field, select Gaia.
5	Enable the applicable Software Blades: <ul style="list-style-type: none"> ▪ On the Network Security tab. ▪ On the Threat Prevention tab.
6	On the Management tab, enable the applicable Software Blades.
7	Click OK .
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 Security Policies .
3	Create a new policy and configure the applicable layers: <ul style="list-style-type: none"> a. At the top, click the + tab (or press CTRL T). b. On the Manage Policies tab, click Manage policies and layers. c. In the Manage policies and layers window, create a new policy and configure the applicable layers. d. Click Close. e. On the Manage Policies tab, click the new policy you created.
4	Create the applicable Access Control 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:

- [R81.20 Security Management Administration Guide](#).
- Applicable *Administration Guides* on the [R81.20 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 199](#)).

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	(1) Licenses and contracts (2) Administrator (3) GUI Clients (4) SNMP Extension (5) Random Pool (6) Certificate Authority (7) Certificate's Fingerprint (8) Automatic start of Check Point Products (9) Exit
Multi-Domain Server, Multi-Domain Log Server	1. mdsenv 2. mdsconfig	(1) Leading VIP Interfaces (2) Licenses (3) Random Pool (4) Groups (5) Certificate's Fingerprint (6) Administrators (7) GUI clients (8) Automatic Start of Multi-Domain Server (9) P1Shell (10) Start Multi-Domain Server Password (11) IPv6 Support for Multi-Domain Server (12) IPv6 Support for Existing Domain Management Servers (13) Exit

Check Point computer	Commands	Available Configuration Options
Security Gateway, Cluster Member	cpconfig	(1) Licenses and contracts (2) SNMP Extension (3) PKCS#11 Token (4) Random Pool (5) Secure Internal Communication (6) Disable cluster membership for this gateway (7) Enable Check Point Per Virtual System State (8) Enable Check Point ClusterXL for Bridge Active/Standby (9) Check Point CoreXL (10) Automatic start of Check Point Products (11) Exit

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

For more information, see the [R81.20 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 R81.20 Gaia Administration Guide - 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).

Menu Option	Description
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.
Automatic start of Check Point Products	Shows and controls which of the installed Check Point products start automatically during boot.
Exit	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 [R81.20 Multi-Domain Security Management Administration Guide](#).

Menu Option	Description
Leading VIP Interfaces	<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>
Licenses	<p>Manages Check Point licenses and contracts on this server.</p>
Random Pool	<p>Configures the RSA keys, to be used by Gaia Operating System.</p>
Groups	<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>
Certificate's Fingerprint	<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>
Administrators	<p>Configures Check Point system administrators for this server.</p>
GUI Clients	<p>Configures the GUI clients that can use SmartConsole to connect to this server.</p>
Automatic Start of Multi-Domain Server	<p>Shows and controls if Multi-Domain Server starts automatically during boot.</p>
P1Shell	<p>Obsolete. Do not use this option anymore.</p> <p> Important - This option and the <code>p1shell</code> command are not supported (Known Limitation PMTR-45085).</p>
Start Multi-Domain Server Password	<p>Configures a password to control the start of the Multi-Domain Server.</p>

Menu Option	Description
IPv6 Support for Multi-Domain Server	Enables or disables the IPv6 Support on the Multi-Domain Server.  Important - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).
IPv6 Support for Existing Domain Management Servers	Enables or disables the IPv6 Support on the Domain Management Servers.  Important - Multi-Domain Server does not support IPv6 at all (Known Limitation PMTR-14989).
Exit	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
Licenses and contracts	Manages Check Point licenses and contracts on this Security Gateway or Cluster Member.
SNMP Extension	Obsolete. Do not use this option anymore. To configure SNMP, see the R81.20 Gaia Administration Guide - Chapter <i>System Management</i> - Section <i>SNMP</i> .
PKCS#11 Token	Register a cryptographic token, for use by Gaia Operating System. See details of the token, and test its functionality.
Random Pool	Configures the RSA keys, to be used by Gaia Operating System.
Secure Internal Communication	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"> ▪ The R81.20 Security Management Administration Guide. ▪ sk65764: How to reset SIC.

Menu Option	Description
Enable cluster membership for this gateway	<p>Enables the cluster membership on the Security Gateway.</p> <p>This change requires a reboot of the Security Gateway. For more information, see the R81.20 ClusterXL Administration Guide.</p> <p>Note - This section does not apply to Scalable Platforms (Maestro and Chassis).</p>
Disable cluster membership for this gateway	<p>Disables the cluster membership on the Security Gateway.</p> <p>This change requires a reboot of the Security Gateway. For more information, see the R81.20 ClusterXL Administration Guide.</p> <p>Note - This section does not apply to Scalable Platforms (Maestro and Chassis).</p>
Enable Check Point Per Virtual System State	<p>Enables Virtual System Load Sharing on the VSX Cluster Member.</p> <p>For more information, see the R81.20 VSX Administration Guide.</p> <p>Note - This section does not apply to Scalable Platforms (Maestro and Chassis).</p>
Disable Check Point Per Virtual System State	<p>Disables Virtual System Load Sharing on the VSX Cluster Member.</p> <p>For more information, see the R81.20 VSX Administration Guide.</p> <p>Note - This section does not apply to Scalable Platforms (Maestro and Chassis).</p>
Enable Check Point ClusterXL for Bridge Active/Standby	<p>Enables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the R81.20 ClusterXL Administration Guide.</p> <p>Note - This section does not apply to Scalable Platforms (Maestro and Chassis).</p>
Disable Check Point ClusterXL for Bridge Active/Standby	<p>Disables Check Point ClusterXL for Bridge mode. This change requires a reboot of the Cluster Member. For more information, see the R81.20 ClusterXL Administration Guide.</p> <p>Note - This section does not apply to Scalable Platforms (Maestro and Chassis).</p>

Menu Option	Description
Check Point CoreXL	<p>Manages CoreXL and Firewall mode on the Security Gateway / Cluster Member / Scalable Platform Security Group.</p> <p>After all changes in CoreXL configuration, you must reboot the Security Gateway / Cluster Member / Security Group.</p> <p>For more information, see the R81.20 Performance Tuning Administration Guide.</p>
Automatic start of Check Point Products	<p>Shows and controls which of the installed Check Point products start automatically during boot.</p>
Exit	<p>Exits from the Check Point Configuration Tool.</p>

Installing Software Packages on Gaia

You can install Software Packages in these ways on Gaia R81.20:

Installing Software Packages centrally on Security Gateways and Cluster Members

These options are available on an R81.20 Management Server:

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

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 [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.



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](#).

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"> 1. Connect to the Gaia Portal or Gaia Clish on your Gaia computer. 2. Verify the applicable CPUSE Software Packages. 3. Download the applicable CPUSE Software Packages. 4. Install the applicable CPUSE Software Packages.
Offline	See the instructions for a Gaia computer that is not connected to the Internet.

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

Installation Method	Action Plan
Offline only	<p>Installation in Gaia Portal</p> <ol style="list-style-type: none"> 1. Use the computer, from which you connect to Gaia Portal. 2. Download the applicable CPUSE Software Packages from the R81.20 Home Page. 3. Connect to Gaia Portal on your Gaia computer. 4. Import the applicable CPUSE Software Packages. 5. Verify the applicable CPUSE Software Packages. 6. Install the applicable CPUSE Software Packages. <p>Installation in Gaia Clish</p> <ol style="list-style-type: none"> 1. Use the computer, from which you connect to Gaia Portal. 2. Download the applicable CPUSE Software Packages from the R81.20 Home Page. 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>). 4. Connect to Gaia Clish on your Gaia computer. 5. Import the applicable CPUSE Software Packages. 6. Verify the applicable CPUSE Software Packages. 7. Install the applicable CPUSE Software Packages.

 **Important:**

When you perform an upgrade to R81.20 with CPUSE from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions, 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 R81.20 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

Upgrade Options and Prerequisites

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

-  **Note** - Download the applicable installation and upgrade images in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

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 [R81.20 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 [R81.20 Known Limitations SK](#).
- When you use the **Advanced Upgrade** or the **Migration and Upgrade** method, **before** you import the management database on the R81.20 Servers, we strongly recommend to install the latest Recommended Take of the [R81.20 Jumbo Hotfix Accumulator](#).

This makes sure the R81.20 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 R81.20 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 (see ["Contract Verification" on page 220](#)).

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 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.

- Collect the Log Exporter configuration - see [sk127653](#).
- 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/
- On your Security Management Servers, Multi-Domain Servers, Domain Management Servers, Multi-Domain Log Servers, Domain Log Servers, Log Servers, and SmartEvent Servers:

Starting in R81.20, when you upgrade a Management Server / Log Server to a new version, log file migration to the new version is limited to logs for the past 180 days.

You can change the age of log files to a number between 30 and 360 days.

Procedure

1. Connect to the command line on the server (Security Management Server, Multi-Domain Server, Multi-Domain Log Server, dedicated Log Server, dedicated SmartEvent Server):
2. Log in to the Expert mode.
3. Create the required XML file:

```
touch $FWDIR/conf/upgradeLogData.xml
```

4. Edit this XML file:

```
vi $FWDIR/conf/upgradeLogData.xml
```

5. This XML file must contain these lines:

```
<?xml version="1.0"?>
  <config>
    <ImportLogDays>NUMBER_OF_DAYS</ImportLogDays>
  </config>
```

The number of days must be an integer between 30 and 360.

6. Save the changes in the file and exit the editor.

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

Action Plan for Security Management Servers in High Availability

- i 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 R81.20	Action Plan
From R80.20, R80.20.M2, and higher versions	<ol style="list-style-type: none"> 1. Upgrade the Primary Security Management Server. 2. Make sure the Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794. 3. Upgrade the Secondary Security Management Servers.
From R80.20.M1 version	<ol style="list-style-type: none"> 1. Upgrade the Primary Security Management Server. 2. Perform a clean install of the Secondary Security Management Servers. 3. Connect the Secondary Security Management Servers to the Primary Security Management Server.


Action Plan for Multi-Domain Servers in High Availability

- i 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 R81.20	Action Plan
From R80.20, R80.20.M2, and higher versions	<ol style="list-style-type: none"> 1. Make sure to run Pre-Upgrade Verifier on all source servers and to fix all detected issues before you start the upgrade. 2. Make sure the Global Domain is Active on the Primary Multi-Domain Server. 3. Upgrade the Primary Multi-Domain Server. 4. Make sure the Multi-Domain Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794. 5. Upgrade the Secondary Multi-Domain Servers.
From R80.20.M1 version	<ol style="list-style-type: none"> 1. Make sure to run Pre-Upgrade Verifier on all source servers and to fix all detected issues before you start the upgrade. 2. Make sure the Global Domain is Active on the Primary Multi-Domain Server. 3. Upgrade the Primary Multi-Domain Server. 4. Perform a clean install of the Secondary Multi-Domain Servers. 5. Connect the Secondary Multi-Domain Servers to the Primary Multi-Domain Server.

- 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	Delete all unused Threat Prevention Profiles on the Global Domain: <ol style="list-style-type: none"> Connect with SmartConsole to the Global Domain. From the left navigation panel, click Security Policies. Open each policy. In the top section, click Threat Prevention. In the bottom section Custom Policy Tools, click Profiles. Delete all unused Threat Prevention Profiles. Publish the SmartConsole session. Close SmartConsole.
2	Disable the Staging Mode for IPS protections (see sk142432): <ol style="list-style-type: none"> Connect with SmartConsole to each Domain. From the left navigation panel, click Security Policies. Open each policy. In the top section, click Threat Prevention. In the bottom section Custom Policy Tools, click Profiles. Edit each profile. From the left tree, click IPS > Updates. Clear the box Set activation as staging mode (Detect). Click OK. Publish the SmartConsole session. Close SmartConsole.

- 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 a different interface as the Leading interface after the upgrade, see [sk107336](#).
- If an external storage device is connected to a Management Server or Log Server, you must follow [sk66003](#).

Action Plan

1. Unmount and disconnect the external storage device.
2. Upgrade the server to R81.20.
3. Stop the SOLR process.
4. Connect and mount the external storage device to the server.
5. On the external storage device, configure the required settings to keep log indexes.
6. Start the SOLR process.

Required Disk Space:

- The size of the `/var/log/` partition on the target Management Server or Log Server must be at minimum 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 minimum 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. It is possible to change this configuration after the upgrade or migration.

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](#) for links).
- See the [R81.20 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 [R81.20 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/fwkernel.conf
- \$FWDIR/boot/modules/vpnkernel.conf
- \$FWDIR/conf/fwaffinity.conf
- \$FWDIR/conf/fwauthd.conf
- \$FWDIR/conf/local.arp
- \$FWDIR/conf/discntd.if
- \$FWDIR/conf/cpha_bond_ls_config.conf
- \$FWDIR/conf/resctrl
- \$FWDIR/conf/vsaffinity_exception.conf
- \$FWDIR/database/qos_policy.C
- \$PPKDIR/conf/simkernel.conf:
- \$PPKDIR/conf/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/fwkernel.conf
- \$FWDIR/boot/modules/vpnkernel.conf
- \$FWDIR/conf/fwaffinity.conf
- \$FWDIR/conf/fwauthd.conf
- \$FWDIR/conf/local.arp

- `$FWDIR/conf/discntd.if`
- `$FWDIR/conf/cpha_bond_ls_config.conf`
- `$FWDIR/conf/resctrl`
- `$FWDIR/conf/vsaffinity_exception.conf`
- `$FWDIR/database/qos_policy.C`
- `$PPKDIR/conf/simkern.conf`
- `$PPKDIR/conf/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 (see "[Contract Verification](#)" on page 220).

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

i Important - If you use the Mobile Access Software Blade and you have customized configuration, review the customized settings **before** you upgrade to R81.20. 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 [R81.20 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 [R81.20 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 (see ["Contract Verification" on page 220](#)).

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	Open these files on the Management Server and write down all custom changes in the applicable files:

Step	Instructions
	<ul style="list-style-type: none"> ▪ Mobile Access configuration: \$CVPNDIR/conf/cvpnd.C
	<ul style="list-style-type: none"> ▪ Apache configuration: \$CVPNDIR/conf/httpd.conf \$CVPNDIR/conf/includes/*
	<ul style="list-style-type: none"> ▪ Local certificates: \$CVPNDIR/var/ssl/ca-bundle/*
	<ul style="list-style-type: none"> ▪ DynamicID - SMS OTP - Local Phone List: \$CVPNDIR/conf/SmsPhones.lst
	<ul style="list-style-type: none"> ▪ RSA configuration: /var/ace/sdconf.rec
	<ul style="list-style-type: none"> ▪ 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 {} \;</pre> <pre>find \$CVPNDIR/ -name *.gif -type f -exec ls {} \;</pre> <pre>find \$CVPNDIR/ -name *.jpg -type f -exec ls {} \;</pre>
2	Upgrade the Management Server to R81.20 using one of the supported methods (see " Upgrade Methods " on page 215).
3	<p>Update the Mobile Access Endpoint Compliance:</p> <ol style="list-style-type: none"> 1. In SmartConsole, from the left navigation panel, click Security Policies. 2. In the Shared Policies section, click Mobile Access > Open Mobile Access Policy in SmartDashboard. 3. In SmartDashboard, click Mobile Access tab > open Endpoint Security on Demand > click Endpoint Compliance Updates > click Update Databases Now. 4. Close SmartDashboard.
4	Manually edit the default files on the upgraded the Management Server to include your custom changes.

Upgrade Methods

You can use these methods to upgrade your Security Gateways and Cluster Members:

Gateway	Central Deployment	Central Deployment Tool	CPUSE
Security Gateways, VSX Gateways, Cluster Members	See "Upgrade of Security Gateways and Cluster Members with Central Deployment" on the next page  Best Practice - Use this method.	See "Upgrade of Security Gateways and Cluster Members with Central Deployment Tool" on page 217	See "Upgrade with CPUSE" on page 217

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

Server	CPUSE	Advanced Upgrade	Migration and Upgrade
Security Management Server, Endpoint Security Management Server, CloudGuard Controller	See "Upgrade with CPUSE" on page 217	See "Advanced Upgrade of Management Servers and Log Servers" on page 218	See "Migration and Upgrade of Management Servers and Log Servers" on page 219
Multi-Domain Server	See "Upgrade with CPUSE" on page 217	See "Advanced Upgrade of Management Servers and Log Servers" on page 218	See "Migration and Upgrade of Management Servers and Log Servers" on page 219

Server	CPUSE	Advanced Upgrade	Migration and Upgrade
Multi-Domain Log Server	See "Upgrade with CPUSE" on the next page	See "Advanced Upgrade of Management Servers and Log Servers" on page 218	See "Migration and Upgrade of Management Servers and Log Servers" on page 219
Dedicated Log Server, Endpoint Policy Server	See "Upgrade with CPUSE" on the next page	See "Advanced Upgrade of Management Servers and Log Servers" on page 218	See "Migration and Upgrade of Management Servers and Log Servers" on page 219
Dedicated SmartEvent Server	See "Upgrade with CPUSE" on the next page	See "Advanced Upgrade of Management Servers and Log Servers" on page 218	See "Migration and Upgrade of Management Servers and Log Servers" on page 219

 **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.
- 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

With Central Deployment in SmartConsole, you can install software packages to upgrade or to perform a clean install on Security Gateways and Cluster Members.

You can Deploy a Hotfix or Upgrade 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 [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.



Best Practice - Use this method.

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 for Management Servers and Log Servers, see:

- ["Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE" on page 225](#)
- ["Upgrading one Multi-Domain Server from R80.20 and higher" on page 261](#)
- ["Upgrading Multi-Domain Servers in High Availability from R80.20 and higher" on page 289](#)
- ["Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE" on page 351](#)
- ["Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE" on page 371](#)



Note - When you perform an upgrade to R81.20 with CPUSE from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions, you can see the upgrade report in Gaia Portal. See ["Installing Software Packages on Gaia" on page 199](#).

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 R81.20 Management Server Migration Tool.
3	Get the R81.20 Check Point computer: <ul style="list-style-type: none"> ▪ If the current Check Point computer runs on Gaia, you can upgrade it to R81.20. ▪ If the current Check Point computer runs an operating system other than Gaia, you must perform a clean install of the R81.20.
4	Import the entire management database.

For detailed Advanced Upgrade instructions, see:

- ["Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 232](#)
- ["Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade" on page 269](#)
- ["Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade" on page 300](#)
- ["Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade" on page 356](#)
- ["Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade" on page 377](#)

Note - When you perform an upgrade to R81.20 from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions, 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 R81.20 Management Server Migration Tool.
2	Install another target R81.20 Check Point computer.
3	Import the entire management database on the new target R81.20 Check Point computer.

For detailed migration and upgrade instructions, see:

- ["Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration" on page 243](#)
- ["Upgrading one Multi-Domain Server from R80.20 and higher with Migration" on page 279](#)
- ["Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration" on page 325](#)
- ["Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration" on page 363](#)
- ["Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration" on page 388](#)

 **Note** - When you perform an upgrade to R81.20 from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions, 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
```

Contract Verification

Before you upgrade your Management Server to R81.20, 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 Check Point User Center account, download a Contract File directly from your User Center account:
Import a local contract file	If the Management Server does not have Internet access: <ol style="list-style-type: none"> 1. On a computer with Internet access, log in to your Check Point User Center account. 2. In the top menu, click Assets/Info > Download Contract File and follow the instructions on the screen. 3. Transfer the downloaded contract file to your Management Server. 4. Select Import a local contracts file. 5. Enter the full path to the location where you stored the contract file.

Option	Instructions
Continue without contract information	<p>Select this option, if you intend to get and install a valid Contract File later.</p> <p>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>

Upgrade Tools

 **Important** - You must always use the latest version of the R81.20 Upgrade Tools from [sk135172](#) to:

- Upgrade from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions
- 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.

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 Upgrade Tools package:

Package	Instructions
<code>migrate_server</code>	Exports and imports the management database and applicable Check Point configuration. For details, see the R81.20 CLI Reference Guide > Chapter <i>Security Management Server Commands</i> > Section <i>migrate_server</i> .
<code>migrate.conf</code>	Contains configuration settings for Advanced Upgrade / Database Migration.

Upgrade of Security Management Servers and Log Servers

This section provides instructions to upgrade Security Management Servers and dedicated Log Servers from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions:

- *"Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE" on page 225*
- *"Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 232*
- *"Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration" on page 243*
- *"Upgrading Security Management Servers in Management High Availability from R80.20 and higher" on page 254*

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, R80.30, or higher versions.
- 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 <i>"Backing Up and Restoring" on page 17</i>).
2	See the <i>"Upgrade Options and Prerequisites" on page 202</i> .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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 data-bbox="432 875 1458 972">cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre data-bbox="432 1216 1458 1402">[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>

i 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. Create the required JSON configuration file

i Important:

- If none of the servers in the same Security Management environment changed their original IP addresses, then you do **not** need to create the special JSON configuration file.
Skip this step.
- 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.
You must use the same JSON configuration file on all servers (including Log Servers and SmartEvent Servers) in the same Security Management environment.

To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address.</p> <p>Format for migrating a single Log Server / SmartEvent Server to a new IP address:</p> <pre>[{"name": "<Name of Log Server / SmartEvent Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Log Server / SmartEvent Server>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Security Management environment - the Security Management Server and the Log Server. The Security Management Server remains with the original IP address. The Log Server migrates to a new IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Log Server is: 192.168.10.21 The name of the source R80.30 Log Server object in SmartConsole is: MyLogServer The new IPv4 address of the target R81.20 Log Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Security Management Server and on the Log Server: [{"name": "MyLogServer", "newIpAddress4": "172.30.40.51"}] <p> Important - All servers in this environment must get the same configuration file.</p>

3. Upgrade the Security Management Server with CPUSE


See ["Installing Software Packages on Gaia" on page 199](#) and follow the applicable action plan.

4. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

5. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

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

 **Important** - If this 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.

Follow the applicable procedure in ["Upgrade of Security Management Servers and Log Servers" on page 224](#).

6. Update the object version of the dedicated Log Servers and SmartEvent Servers

i 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 R81.20 Security Management Server that manages the dedicated Log Server or SmartEvent Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the object of the dedicated Log Server or SmartEvent Server.
4	From the left tree, click General Properties .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

7. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server.
2	In the top left corner, click Menu > Install database .
3	Select all objects.
4	Click Install .
5	Click OK .


8. Install the Event Policy

i Important - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R81.20 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R81.20 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click Logs & Monitor .
3	At the top, click + to open a new tab.

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

9. In SmartConsole, install policy on all SmartLSM Security Profiles

 **Important** - This step applies only if you enabled the SmartProvisioning Software Blade on this Management Server.

Step	Instructions
1	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

10. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R81.20 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 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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 data-bbox="432 875 1458 972">cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre data-bbox="432 1216 1458 1400">[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>


i 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.
3	Go to the <code>\$FWDIR/scripts/</code> directory: <pre data-bbox="432 465 1458 528">cd \$FWDIR/scripts</pre>
4	Run the Pre-Upgrade Verifier. <ul style="list-style-type: none"> ■ If this Security Management Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 689 1458 752">./migrate_server verify -v R81.20</pre> ■ If this Security Management Server is not connected to the Internet, run: <pre data-bbox="512 842 1458 943">./migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i> .
5	Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
6	Export the management database: <ul style="list-style-type: none"> ■ If this Security Management Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1391 1458 1491">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ■ If this Security Management Server is not connected to the Internet, run: <pre data-bbox="512 1581 1458 1715">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i> .


Step	Instructions
7	Calculate the MD5 for the exported database files: <pre>md5sum /<Full Path>/<Name of Database File>.tgz</pre>
8	Transfer the exported databases from the source Security Management Server to an external storage: <pre>/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install a new R81.20 Security Management Server


Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	Perform the clean install in one of these ways (do not perform initial configuration in SmartConsole): <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing One Security Management Server only, or Primary Security Management Server in Management High Availability" on page 66.

-  **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 R81.20 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**.
you must create a special JSON configuration file `mdss.json` that contains **each** server that migrates to a new IP address.
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 R81.20 server

-  **Important** - See ["Upgrade Tools" on page 222](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 . Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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 R81.20 Security Management Server, import the databases

Required JSON configuration file

If you installed the target R81.20 Security Management Server with a different IP address than the source Security Management Server, **you must create a special JSON configuration file before you import the management database** from the source Security Management Server. Note that you have to issue licenses for the new IP address.


i Important:

- If none of the servers in the same 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 Security Management environment.


To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R81.20 Security Management Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address. Format for migrating a single Security Management Server to a new IP address:</p> <pre data-bbox="443 1115 1461 1294">[{"name": "<Name of Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Security Management Server>" }]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Security Management environment - the Security Management Server and the Log Server. The Security Management Server migrates to a new IP address. The Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Security Management Server is: 192.168.10.21 The name of the source R80.30 Security Management Server object in SmartConsole is: MySecMgmtServer The new IPv4 address of the target R81.20 Security Management Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Security Management Server and on the Log Server: [{"name": "MySecMgmtServer", "newIpAddress4": "172.30.40.51"}] <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

 **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line on the R81.20 Security Management Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre data-bbox="467 1608 1458 1671">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 R81.20 Security Management Server, to some directory.</p> <p> Note - 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>md5sum /<Full Path>/<Name of Database File>.tgz</pre>
6	<p>Go to the <code>\$FWDIR/scripts/</code> directory:</p> <pre>cd \$FWDIR/scripts/</pre>
7	<p>Import the management database:</p> <ul style="list-style-type: none"> ▪ If this Security Management Server is connected to the Internet, run: <pre>./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ▪ If this Security Management Server is not connected to the Internet, run: <pre>./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>i Important - The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands).</p> <p>For details, see the R81.20 CLI Reference Guide - Chapter Security Management Server Commands - Section <code>migrate_server</code>.</p>

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Install the new licenses

i Important - This step applies only if the target R81.20 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 Check Point User Center account.

Step	Instructions
2	Install the new licenses on the R81.20 Security Management 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 Security Management Server to detect the new licenses. Alternatively, restart Check Point services:
	<pre>cpstop cpstart</pre>

8. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

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

i Important - If this 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.

Follow the applicable procedure in ["Upgrade of Security Management Servers and Log Servers" on page 224](#).

9. Update the object version of the dedicated Log Servers and SmartEvent Servers


i 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 R81.20 Security Management Server that manages the dedicated Log Server or SmartEvent Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the object of the dedicated Log Server or SmartEvent Server.
4	From the left tree, click General Properties .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server.
2	In the top left corner, click Menu > Install database .
3	Select all objects.
4	Click Install .
5	Click OK .

11. Install the Event Policy

 **Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R81.20 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R81.20 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click Logs & Monitor .
3	At the top, click + to open a new tab.
4	In the bottom left corner, in the External Apps section, click SmartEvent Settings & Policy . The Legacy SmartEvent client opens.
5	In the top left corner, click Menu > Actions > Install Event Policy .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click Close .
9	Close the Legacy SmartEvent client.

12. In SmartConsole, install policy on all SmartLSM Security Profiles

i Important - This step applies only if you enabled the SmartProvisioning Software Blade on this Management Server.

Step	Instructions
1	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

13. Test the functionality on the R81.20 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- These instructions equally apply to:
 - 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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: <div data-bbox="432 871 1458 972" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> </div> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <div data-bbox="432 1211 1458 1400" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre> </div>

i 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.
3	Go to the <code>\$FWDIR/scripts/</code> directory: <pre data-bbox="432 465 1458 528">cd \$FWDIR/scripts</pre>
4	Run the Pre-Upgrade Verifier. <ul style="list-style-type: none"> ■ If this Security Management Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 689 1458 752">./migrate_server verify -v R81.20</pre> ■ If this Security Management Server is not connected to the Internet, run: <pre data-bbox="512 842 1458 949">./migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i> .
5	Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
6	Export the management database: <ul style="list-style-type: none"> ■ If this Security Management Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1391 1458 1491">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ■ If this Security Management Server is not connected to the Internet, run: <pre data-bbox="512 1581 1458 1715">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i> .


Step	Instructions
7	<p>Calculate the MD5 for the exported database files:</p> <pre>md5sum /<Full Path>/<Name of Database File>.tgz</pre>
8	<p>Transfer the exported databases from the source Security Management Server to an external storage:</p> <pre>/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install a new R81.20 Security Management Server


Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install in one of these ways (do not perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing One Security Management Server only, or Primary Security Management Server in Management High Availability" on page 66.

-  **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 R81.20 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**.
you must create a special JSON configuration file `mdss.json` that contains **each** server that migrates to a new IP address.
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 R81.20 server

-  **Important** - See ["Upgrade Tools" on page 222](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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 data-bbox="432 595 1458 696">cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre data-bbox="432 936 1458 1122">[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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 R81.20 Security Management Server, import the databases

Required JSON configuration file

If you installed the target R81.20 Security Management Server with a different IP address than the source Security Management Server, **you must create a special JSON configuration file before you import the management database** from the source Security Management Server. Note that you have to issue licenses for the new IP address.


i Important:

- If none of the servers in the same 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 Security Management environment.


To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R81.20 Security Management Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address. Format for migrating a single Security Management Server to a new IP address:</p> <pre data-bbox="443 1115 1460 1294">[{"name": "<Name of Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Security Management Server>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Security Management environment - the Security Management Server and the Log Server. The Security Management Server migrates to a new IP address. The Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Security Management Server is: 192.168.10.21 The name of the source R80.30 Security Management Server object in SmartConsole is: MySecMgmtServer The new IPv4 address of the target R81.20 Security Management Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Security Management Server and on the Log Server: [{"name": "MySecMgmtServer", "newIpAddress4": "172.30.40.51"}] <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

 **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line on the R81.20 Security Management Server.
2	Log in to the Expert mode.
3	<p>Make sure a valid license is installed:</p> <pre data-bbox="467 1608 1460 1671">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 R81.20 Security Management Server, to some directory.</p> <p> Note - 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>md5sum /<Full Path>/<Name of Database File>.tgz</pre>
6	<p>Go to the <code>\$FWDIR/scripts/</code> directory:</p> <pre>cd \$FWDIR/scripts/</pre>
7	<p>Import the management database:</p> <ul style="list-style-type: none"> ▪ If this Security Management Server is connected to the Internet, run: <pre>./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ▪ If this Security Management Server is not connected to the Internet, run: <pre>./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>i Important - The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands).</p> <p>For details, see the R81.20 CLI Reference Guide - Chapter Security Management Server Commands - Section <code>migrate_server</code>.</p>

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Install the new licenses

i **Important** - This step applies only if the target R81.20 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 Check Point User Center account.

Step	Instructions
2	Install the new licenses on the R81.20 Security Management 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 Security Management Server to detect the new licenses. Alternatively, restart Check Point services:
	<pre>cpstop cpstart</pre>

8. Upgrade the dedicated Log Servers and dedicated SmartEvent Servers

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

i Important - If this 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.

Follow the applicable procedure in ["Upgrade of Security Management Servers and Log Servers" on page 224](#).

9. Update the object version of the dedicated Log Servers and SmartEvent Servers


i 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 R81.20 Security Management Server that manages the dedicated Log Server or SmartEvent Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the object of the dedicated Log Server or SmartEvent Server.
4	From the left tree, click General Properties .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server.
2	In the top left corner, click Menu > Install database .
3	Select all objects.
4	Click Install .
5	Click OK .

11. Install the Event Policy

 **Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R81.20 Security Management Server.

Step	Instructions
1	Connect with the SmartConsole to the R81.20 Security Management Server.
2	In the SmartConsole, from the left navigation panel, click Logs & Monitor .
3	At the top, click + to open a new tab.
4	In the bottom left corner, in the External Apps section, click SmartEvent Settings & Policy . The Legacy SmartEvent client opens.
5	In the top left corner, click Menu > Actions > Install Event Policy .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click Close .
9	Close the Legacy SmartEvent client.

12. In SmartConsole, install policy on all SmartLSM Security Profiles

i Important - This step applies only if you enabled the SmartProvisioning Software Blade on this Management Server.

Step	Instructions
1	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

13. Test the functionality on the R81.20 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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 Primary Security Management Server with one of the supported methods.</p> <ul style="list-style-type: none"> ▪ CPUSE See <i>"Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE" on page 225</i> ▪ Advanced Upgrade See <i>"Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 232</i> ▪ Migration See <i>"Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration" on page 243</i>
2	<p>Upgrade the Secondary Security Management Server with one of the supported methods.</p> <p> Important:</p> <ul style="list-style-type: none"> ▪ Make sure the Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794. ▪ If you upgraded the Primary Security Management Server and changed its IPv4 address before you upgrade the Secondary Security Management Server, then you must put the required JSON file on the Secondary Security Management Server. See the corresponding section below. <ul style="list-style-type: none"> ▪ CPUSE See <i>"Upgrading a Security Management Server or Log Server from R80.20 and higher with CPUSE" on page 225</i> ▪ Advanced Upgrade See <i>"Upgrading a Security Management Server or Log Server from R80.20 and higher with Advanced Upgrade" on page 232</i> ▪ Migration See <i>"Upgrading a Security Management Server or Log Server from R80.20 and higher with Migration" on page 243</i>
3	<p>Get the R81.20 SmartConsole. See <i>"Installing SmartConsole" on page 106</i>.</p>
4	<p>Connect with SmartConsole to the R81.20 Primary Security Management Server.</p>

Step	Instructions
5	<p>Update the object version of the Secondary Security Management Server:</p> <ol style="list-style-type: none"> From the left navigation panel, click Gateways & Servers. Open the Secondary Security Management Server object. From the left tree, click General Properties. In the Platform section > in the Version field, select R81.20. Click OK.
6	<p>Make sure Secure Internal Communication (SIC) works correctly with the Secondary Security Management Server:</p> <ol style="list-style-type: none"> From the left navigation panel, click Gateways & Servers. Open the Secondary Security Management Server object. On the General Properties page, click Communication. Click Test SIC Status. The SIC Status must show Communicating. Click Close. Click OK.
7	<p>Upgrade the dedicated Log Servers and SmartEvent Servers. Follow the applicable procedure in "Upgrade of Security Management Servers and Log Servers" on page 224.</p> <p> Important - If you changed the IPv4 address of one or more Security Management Servers during their upgrade, then you must put the required JSON file on the dedicated Log Servers and SmartEvent Servers. See the corresponding section below.</p>
8	<p>Install the management database:</p> <ol style="list-style-type: none"> In the top left corner, click Menu > Install database. Select all objects. Click Install. Click OK.

Step	Instructions
9	<p>Install the Event Policy.</p> <p> Important - This step applies only if the SmartEvent Correlation Unit Software Blade is enabled on the R81.20 Security Management Server.</p> <ol style="list-style-type: none"> In the SmartConsole, from the left navigation panel, click Logs & Monitor. At the top, click + to open a new tab. In the bottom left corner, in the External Apps section, click SmartEvent Settings & Policy. The Legacy SmartEvent client opens. In the top left corner, click Menu > Actions > Install Event Policy. Confirm. Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded Click Close. Close the Legacy SmartEvent client.
10	<p>Synchronize the Security Management Servers:</p> <ol style="list-style-type: none"> In the top left corner, click Menu > Management High Availability. In the Peers section, click Actions > Sync Peer. The status must show Successfully synced for all peers.

Required JSON configuration file

If you installed the target R81.20 Security Management Server with a different IP address than the source Security Management Server, **you must create a special JSON configuration file before you import the management database** from the source Security Management Server. Note that you have to issue licenses for the new IP address.


Important:

- If none of the servers in the same 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 Security Management environment.

To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R81.20 Security Management Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address.</p> <p>Format for migrating only the Primary Security Management Server to a new IP address</p> <pre>[{"name": "<Name of Primary Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Security Management Server"}</pre> <p>Format for migrating both the Primary and the Secondary Security Management Server to new IP addresses</p> <pre>[{"name": "<Name of Primary Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Security Management Server"}, {"name": "<Name of Secondary Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Security Management Server"}</pre> <p>Format for migrating both the Primary and the Secondary Security Management Servers, and the Log Server to new IP addresses</p> <pre>[{"name": "<Name of Primary Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Security Management Server"}, {"name": "<Name of Secondary Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Security Management Server"}, {"name": "<Name of Security Management Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Security Management Server"}</pre>

Step	Instructions
	<p>Example</p> <p>There are 3 servers in the R80.30 Security Management environment - the Primary Security Management Server, the Secondary Security Management Server, and the Log Server. Both the Primary and the Secondary Security Management Servers migrate to new IP addresses. The Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source Primary R80.30 Security Management Server is: 192.168.10.21 The current IPv4 address of the source Secondary R80.30 Security Management Server is: 192.168.10.22 The name of the source Primary R80.30 Security Management Server object in SmartConsole is: MyPrimarySecMgmtServer The name of the source Secondary R80.30 Security Management Server object in SmartConsole is: MySecondarySecMgmtServer The new IPv4 address of the target Primary R81.20 Security Management Server is: 172.30.40.51 The new IPv4 address of the target Secondary R81.20 Security Management Server is: 172.30.40.52 The required syntax for the JSON configuration file you must use on both the Primary and the Secondary Security Management Servers, and on the Log Server: <pre>[{"name": "MyPrimarySecMgmtServer", "newIpAddress4": "172.30.40.51"}, {"name": "MySecondarySecMgmtServer", "newIpAddress4": "172.30.40.52"}]</pre> <p> Important - All servers in this environment must get the same configuration file.</p>

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 R80.20 and higher" on page 261](#)
- ["Upgrading Multi-Domain Servers in High Availability from R80.20 and higher" on page 289](#)
- ["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 350](#)

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, R80.30, or higher versions:

- *"Upgrading one Multi-Domain Server from R80.20 and higher with CPUSE" on page 262*
- *"Upgrading one Multi-Domain Server from R80.20 and higher with Advanced Upgrade" on page 269*
- *"Upgrading one Multi-Domain Server from R80.20 and higher with Migration" on page 279*

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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish the session.
4	<p>If there are Global Policies configured on the Global Domain:</p> <ol style="list-style-type: none"> Connect with SmartConsole to the Global Domain on your source Multi-Domain Server. Reassign all Global Policies to all applicable Domains. <p> Important - Do not publish any changes in the Global Domain until you complete the upgrade to the next available version. This is necessary to avoid any potential issues caused by different policy revisions on the Global Domain and on other Domains.</p>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	<p>Install the latest version of the CPUSE from sk92449.</p> <p>Note - This is to make sure the CPUSE is able to support the required Upgrade Tools package.</p>
7	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
8	<p>In Management High Availability, before you start the upgrade on other servers:</p> <ol style="list-style-type: none"> Make sure the Primary Multi-Domain Server is upgraded and runs. Make sure the Multi-Domain Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794.

Procedure:**1. Get the required Upgrade Tools on the server**

- i Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 . Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>

- i 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. Create the required JSON configuration file

i 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.
Skip this step.
- Even if only one of the servers migrates to a new IP address, all the other servers (including all Multi-Domain Log Servers, Log Servers, and SmartEvent Servers) must get this configuration file.
You must use the same JSON configuration file on all servers (including Multi-Domain Log Servers, 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 Multi-Domain Security Management Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address. Format for migrating a single Log Server / SmartEvent Server to a new IP address:</p> <pre>[{"name": "<Name of Multi-Domain Log Server / Log Server / SmartEvent Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Multi-Domain Log Server / Log Server / SmartEvent Server>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Multi-Domain Security Management environment - the Multi-Domain Server and the Multi-Domain Log Server. The Multi-Domain Server remains with the original IP address. The Multi-Domain Log Server migrates to a new IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Multi-Domain Log Server is: 192.168.10.21 The name of the source R80.30 Multi-Domain Log Server object in SmartConsole is: MyMultiDomainLogServer The new IPv4 address of the target R81.20 Multi-Domain Log Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Multi-Domain Server and on the Multi-Domain Log Server: <pre>[{"name": "MyMultiDomainLogServer", "newIpAddress4": "172.30.40.51"}]</pre> <p> Important - All servers in this environment must get the same configuration file.</p>


3. Upgrade the Multi-Domain Server with CPUSE

See ["Installing Software Packages on Gaia" on page 199](#) and follow the applicable action plan.

4. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

5. 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:

- ["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 350](#)
- ["Upgrade of Security Management Servers and Log Servers" on page 224](#)

6. Reconfigure the User and Device Management Server

i Important - This step applies only if the User and Device Management (UDM) is configured on one of the Domain Management Servers.

Step	Instructions
1	Close all SmartConsole clients connected the R81.20 Multi-Domain Server.
2	Connect to the command line on the R81.20 Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.
5	Go to the main MDS context: <pre data-bbox="432 712 1458 775">mdsenv</pre>
6	Examine the port numbers configured in the file <code>\$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</code> in the attribute " port () ": <pre data-bbox="432 943 1458 999">cat \$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</pre> Example: <pre data-bbox="432 1048 1458 1547"> (: (My_Domain_Management_Server_1 :port (30000) :port_SL (30001) :ip_addr (192.168.2.1)) : (My_Domain_Management_Server_2 :port (30002) :port_SL (30003) :ip_addr (192.168.2.2))) </pre>
7	Configure the same port numbers in the file <code>\$UDMDIR/conf/cmas_list.conf</code> in the attribute " WSPort ": <pre data-bbox="432 1671 1458 1727">vi \$UDMDIR/conf/cmas_list.conf</pre> Example: <pre data-bbox="432 1783 1458 1883"> 192.168.2.1:WSPort=30000:MDSip=192.168.2.254 192.168.2.2:WSPort=30002:MDSip=192.168.2.254 </pre>

Step	Instructions
8	Save the changes in the file and exit the editor.
9	Restart the User and Device Management services: <pre>udmstop ; udmstart</pre>

7. In SmartConsole of each applicable Domain Management Server, install policy on all SmartLSM Security Profiles

i Important - This step applies to each Domain Management Server that manages SmartLSM Security Profiles.

Step	Instructions
1	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

8. Test the functionality on the R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- For additional information related to this upgrade, see [sk163814](#).

i Important - Before you upgrade a Multi-Domain Server:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish the session.
4	<p>If there are Global Policies configured on the Global Domain:</p> <ol style="list-style-type: none"> Connect with SmartConsole to the Global Domain on your source Multi-Domain Server. Reassign all Global Policies to all applicable Domains. <p>i Important - Do not publish any changes in the Global Domain until you complete the upgrade to the next available version. This is necessary to avoid any potential issues caused by different policy revisions on the Global Domain and on other Domains.</p>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	<p>Install the latest version of the CPUSE from sk92449.</p> <p>Note - This is to make sure the CPUSE is able to support the required Upgrade Tools package.</p>
7	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
8	<p>In Management High Availability, before you start the upgrade on other servers:</p> <ol style="list-style-type: none"> Make sure the Primary Multi-Domain Server is upgraded and runs. Make sure the Multi-Domain Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794.

Procedure:

1. Get the required Upgrade Tools on the source server

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.</p> <p>Run this command in the Expert mode:</p> <pre>cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>


i 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"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 539 1461 645">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre data-bbox="512 696 1461 801">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - 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"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
6	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre data-bbox="432 1160 1461 1223">cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1346 1461 1451">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre data-bbox="512 1503 1461 1630">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> <p>For details, see the R81.20 CLI Reference Guide - 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 data-bbox="432 1805 1461 1868">md5sum /<Full Path>/<Name of Database File>.tgz</pre>


Step	Instructions
9	<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: 10px 0;">/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install a new R81.20 Multi-Domain Server

Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install in one of these ways (do not perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 83.

 **Important** - If it is necessary to have a different IP address on the new R81.20 server, you have to issue licenses for the new IP address.

4. Get the required Upgrade Tools on the R81.20 server

 **Important** - See ["Upgrade Tools" on page 222](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 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 data-bbox="432 322 1458 421">cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre data-bbox="459 667 1458 846">[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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 R81.20 Multi-Domain Server, import the databases

Step	Instructions
1	Connect to the command line on the R81.20 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> <pre data-bbox="432 1659 1458 1720">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 R81.20 Multi-Domain Server, to some directory.</p> <p>Note - Make sure to transfer the file in the binary mode.</p>

Step	Instructions
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 data-bbox="432 360 1460 423">md5sum /<Full Path>/<Name of Exported File>.tgz</pre>
7	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre data-bbox="432 506 1460 568">cd \$MDS_FWDIR/scripts/</pre>
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 689 1460 792">./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre data-bbox="512 842 1460 981">./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>For details, see the R81.20 CLI Reference Guide - 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 CPCA) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="432 1227 1460 1290">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="432 1420 1460 1644">mdsstop_customer <IP Address or Name of Domain Management Server> mdsstart_customer <IP Address or Name of Domain Management Server> mdsstat</pre>

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers

i 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:

- ["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 350](#)
- ["Upgrade of Security Management Servers and Log Servers" on page 224](#)

8. Reconfigure the User and Device Management Server

i Important - This step applies only if the User and Device Management (UDM) is configured on one of the Domain Management Servers.

Step	Instructions
1	Close all SmartConsole clients connected the R81.20 Multi-Domain Server.
2	Connect to the command line on the R81.20 Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.
5	Go to the main MDS context: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-top: 5px;">mdsenv</div>

Step	Instructions
6	<p>Examine the port numbers configured in the file <code>\$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</code> in the attribute "port ()":</p> <pre data-bbox="432 360 1458 421">cat \$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</pre> <p>Example:</p> <pre data-bbox="432 472 1458 972">(: (My_Domain_Management_Server_1 :port (30000) :port_SL (30001) :ip_addr (192.168.2.1)) : (My_Domain_Management_Server_2 :port (30002) :port_SL (30003) :ip_addr (192.168.2.2)))</pre>
7	<p>Configure the same port numbers in the file <code>\$UDMDIR/conf/cmas_list.conf</code> in the attribute "WSPort":</p> <pre data-bbox="432 1093 1458 1153">vi \$UDMDIR/conf/cmas_list.conf</pre> <p>Example:</p> <pre data-bbox="432 1205 1458 1308">192.168.2.1:WSPort=30000:MDSip=192.168.2.254 192.168.2.2:WSPort=30002:MDSip=192.168.2.254</pre>
8	<p>Save the changes in the file and exit the editor.</p>
9	<p>Restart the User and Device Management services:</p> <pre data-bbox="432 1464 1458 1525">udmstop ; udmstart</pre>

9. In SmartConsole of each applicable Domain Management Server, install policy on all SmartLSM Security Profiles

Important - This step applies to each Domain Management Server that manages SmartLSM Security Profiles.

Step	Instructions
1	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

10. Test the functionality on the R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish the session.
4	<p>If there are Global Policies configured on the Global Domain:</p> <ol style="list-style-type: none"> Connect with SmartConsole to the Global Domain on your source Multi-Domain Server. Reassign all Global Policies to all applicable Domains. <p> Important - Do not publish any changes in the Global Domain until you complete the upgrade to the next available version. This is necessary to avoid any potential issues caused by different policy revisions on the Global Domain and on other Domains.</p>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	<p>Install the latest version of the CPUSE from sk92449.</p> <p>Note - This is to make sure the CPUSE is able to support the required Upgrade Tools package.</p>
7	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
8	<p>In Management High Availability, before you start the upgrade on other servers:</p> <ol style="list-style-type: none"> Make sure the Primary Multi-Domain Server is upgraded and runs. Make sure the Multi-Domain Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794.

Procedure:**1. Get the required Upgrade Tools on the source server**

- i Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 . Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>


- i 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"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 539 1458 645">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre data-bbox="512 696 1458 801">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - 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"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
6	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre data-bbox="432 1160 1458 1223">cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1346 1458 1451">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre data-bbox="512 1503 1458 1630">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> <p>For details, see the R81.20 CLI Reference Guide - 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 data-bbox="432 1805 1458 1868">md5sum /<Full Path>/<Name of Database File>.tgz</pre>


Step	Instructions
9	<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: 10px 0;">/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install a new R81.20 Multi-Domain Server

Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install in one of these ways (do not perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 83.


 **Important** - If it is necessary to have a different IP address on the new R81.20 server, you have to issue licenses for the new IP address.

4. Get the required Upgrade Tools on the R81.20 server

 **Important** - See ["Upgrade Tools" on page 222](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 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 data-bbox="432 322 1458 423">cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre data-bbox="459 667 1458 848">[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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 R81.20 Multi-Domain Server, import the databases

Step	Instructions
1	Connect to the command line on the R81.20 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> <pre data-bbox="432 1659 1458 1720">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 R81.20 Multi-Domain Server, to some directory.</p> <p> Note - Make sure to transfer the file in the binary mode.</p>

Step	Instructions
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 data-bbox="432 360 1458 423">md5sum /<Full Path>/<Name of Exported File>.tgz</pre>
7	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre data-bbox="432 506 1458 568">cd \$MDS_FWDIR/scripts/</pre>
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 689 1458 792">./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre data-bbox="512 842 1458 981">./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>For details, see the R81.20 CLI Reference Guide - 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 CPCA) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="432 1227 1458 1290">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="432 1420 1458 1644">mdsstop_customer <IP Address or Name of Domain Management Server> mdsstart_customer <IP Address or Name of Domain Management Server> mdsstat</pre>

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers

i 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:

- ["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 350](#)
- ["Upgrade of Security Management Servers and Log Servers" on page 224](#)

8. Reconfigure the User and Device Management Server

i Important - This step applies only if the User and Device Management (UDM) is configured on one of the Domain Management Servers.

Step	Instructions
1	Close all SmartConsole clients connected the R81.20 Multi-Domain Server.
2	Connect to the command line on the R81.20 Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.
5	Go to the main MDS context: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-top: 5px;">mdsenv</div>

Step	Instructions
6	<p>Examine the port numbers configured in the file <code>\$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</code> in the attribute "port ()":</p> <pre data-bbox="432 360 1458 421">cat \$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</pre> <p>Example:</p> <pre data-bbox="432 472 1458 972">(: (My_Domain_Management_Server_1 :port (30000) :port_SL (30001) :ip_addr (192.168.2.1)) : (My_Domain_Management_Server_2 :port (30002) :port_SL (30003) :ip_addr (192.168.2.2)))</pre>
7	<p>Configure the same port numbers in the file <code>\$UDMDIR/conf/cmas_list.conf</code> in the attribute "WSPort":</p> <pre data-bbox="432 1093 1458 1153">vi \$UDMDIR/conf/cmas_list.conf</pre> <p>Example:</p> <pre data-bbox="432 1205 1458 1308">192.168.2.1:WSPort=30000:MDSip=192.168.2.254 192.168.2.2:WSPort=30002:MDSip=192.168.2.254</pre>
8	<p>Save the changes in the file and exit the editor.</p>
9	<p>Restart the User and Device Management services:</p> <pre data-bbox="432 1464 1458 1525">udmstop ; udmstart</pre>

9. In SmartConsole of each applicable Domain Management Server, install policy on all SmartLSM Security Profiles

i Important - This step applies to each Domain Management Server that manages SmartLSM Security Profiles.

Step	Instructions
1	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

10. Test the functionality on the R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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 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, R80.30, or higher versions:

- ["Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with CPUSE" on page 290](#)
- ["Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Advanced Upgrade" on page 300](#)
- ["Upgrading Multi-Domain Servers in High Availability from R80.20 and higher with Migration" on page 325](#)
- ["Managing Domain Management Servers During the Upgrade Process" on page 349](#)

For additional information related to these upgrade procedures, see [sk163814](#).

For configuration information, see the [R81.20 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, R80.30, or higher versions.
- For additional information related to this upgrade, see [sk163814](#).

i Important - Before you upgrade Multi-Domain Servers:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish the session.
4	If there are Global Policies configured on the Global Domain: <ol style="list-style-type: none"> Connect with SmartConsole to the Global Domain on your source Multi-Domain Server. Reassign all Global Policies to all applicable Domains. <p>i Important - Do not publish any changes in the Global Domain until you complete the upgrade to the next available version. This is necessary to avoid any potential issues caused by different policy revisions on the Global Domain and on other Domains.</p>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	Install the latest version of the CPUSE from sk92449 . Note - This is to make sure the CPUSE is able to support the required Upgrade Tools package.
7	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
8	In Management High Availability, before you start the upgrade on other servers: <ol style="list-style-type: none"> Make sure the Primary Multi-Domain Server is upgraded and runs. Make sure the Multi-Domain Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794.

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

Procedure:

1. If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary

For instructions, see the [R81.20 Multi-Domain Security Management Administration Guide](#) - Chapter *Working with High Availability* - Section *Failure Recovery* - Subsection *Promoting the Secondary Multi-Domain Server to Primary*.

2. Make sure the Global Domain is Active on the Primary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the Primary Multi-Domain Server.
2	<p>From the left navigation panel, click Multi Domain > Domains. The table shows Domains and Multi-Domain Servers:</p> <ul style="list-style-type: none"> ▪ 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.
3	<p>In the leftmost column Domains, examine the bottom row Global for the Primary Multi-Domain Server. If the Global Domain is in the Standby state on the Primary Multi-Domain Server (marked with an empty "barrel" icon), then make it Active:</p> <ol style="list-style-type: none"> a. Right-click on the Primary Multi-Domain Server and click Connect to Domain Server. The High Availability Status window opens. b. In the section Connected To, click Actions > Set Active. c. Click Yes to confirm. d. Wait for the full synchronization to complete. e. Close SmartConsole.

3. Get the required Upgrade Tools on the Primary Multi-Domain Server

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.</p> <p>Run this command in the Expert mode:</p> <pre> cprood_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre> [Expert@HostName:0]# cprood_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre>

i 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. Create the required JSON configuration file on the Primary Multi-Domain Server

i 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.
Skip this step.
- Even if only one of the servers migrates to a new IP address, all the other servers (including all Multi-Domain Log Servers, Log Servers, and SmartEvent Servers) must get this configuration file.
You must use the same JSON configuration file on all servers (including the Secondary Multi-Domain Servers, Multi-Domain Log Servers, 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 Primary Multi-Domain Security Management Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address. Format for migrating a Secondary Multi-Domain Server / Multi-Domain Log Server / Log Server / SmartEvent Server to a new IP address:</p> <pre>[{"name": "<Name of Server #1 Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Server #1>"}, {"name": "<Name of Server #2 Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Server #2>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Multi-Domain Security Management environment - the Multi-Domain Server and the Multi-Domain Log Server. The Multi-Domain Server remains with the original IP address. The Multi-Domain Log Server migrates to a new IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Multi-Domain Log Server is: 192.168.10.21 The name of the source R80.30 Multi-Domain Log Server object in SmartConsole is: MyMultiDomainLogServer The new IPv4 address of the target R81.20 Multi-Domain Log Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Multi-Domain Server and on the Multi-Domain Log Server: <pre>[{"name": "MyMultiDomainLogServer", "newIpAddress4": "172.30.40.51"}]</pre> <p> Important - All servers in this environment must get the same configuration file.</p>


5. Upgrade the Primary Multi-Domain Server with CPUSE


See ["Installing Software Packages on Gaia" on page 199](#) and follow the applicable action plan.

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. 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 ["Upgrade Tools" on page 222](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>

Step	Instructions
2	<p>Install the R81.20 Upgrade Tools with CPUSE. See "Installing Software Packages on Gaia" on page 199 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-R81.20 BuildNumber 1 </pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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.
    
```

8. Upgrade the Secondary Multi-Domain Server with CPUSE

See ["Installing Software Packages on Gaia" on page 199](#) and follow the applicable action plan.

9. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Primary Multi-Domain Server.
2	From the left navigation panel, click Multi-Domain > Domains .
3	From the top toolbar, open the Secondary Multi-Domain Server object.

Step	Instructions
4	From the left tree, click General .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

10. Upgrade the Multi-Domain Log Servers, dedicated Log Servers, and dedicated SmartEvent Servers

- i 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:

- ["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 350](#)
- ["Upgrade of Security Management Servers and Log Servers" on page 224](#)

11. Reconfigure the User and Device Management Server

- i Important** - This step applies only if the User and Device Management (UDM) is configured on one of the Domain Management Servers.

Step	Instructions
1	Close all SmartConsole clients connected the R81.20 Multi-Domain Server.
2	Connect to the command line on the R81.20 Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.
5	Go to the main MDS context: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-top: 5px;"> <pre>mdsenv</pre> </div>

Step	Instructions
6	<p>Examine the port numbers configured in the file <code>\$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</code> in the attribute "port ()":</p> <pre data-bbox="432 360 1458 421">cat \$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</pre> <p>Example:</p> <pre data-bbox="432 472 1458 972">(: (My_Domain_Management_Server_1 :port (30000) :port_SL (30001) :ip_addr (192.168.2.1)) : (My_Domain_Management_Server_2 :port (30002) :port_SL (30003) :ip_addr (192.168.2.2)))</pre>
7	<p>Configure the same port numbers in the file <code>\$UDMDIR/conf/cmas_list.conf</code> in the attribute "WSPort":</p> <pre data-bbox="432 1093 1458 1153">vi \$UDMDIR/conf/cmas_list.conf</pre> <p>Example:</p> <pre data-bbox="432 1205 1458 1308">192.168.2.1:WSPort=30000:MDSip=192.168.2.254 192.168.2.2:WSPort=30002:MDSip=192.168.2.254</pre>
8	<p>Save the changes in the file and exit the editor.</p>
9	<p>Restart the User and Device Management services:</p> <pre data-bbox="432 1464 1458 1525">udmstop ; udmstart</pre>

12. In SmartConsole of each applicable Domain Management Server, install policy on all SmartLSM Security Profiles

Important - This step applies to each Domain Management Server that manages SmartLSM Security Profiles.

Step	Instructions
1	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

13. Test the functionality on the Primary R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the Primary R81.20 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, R80.30, or higher versions.
- For additional information related to this upgrade, see [sk163814](#).

i Important - Before you upgrade Multi-Domain Servers:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish the session.
4	<p>If there are Global Policies configured on the Global Domain:</p> <ol style="list-style-type: none"> Connect with SmartConsole to the Global Domain on your source Multi-Domain Server. Reassign all Global Policies to all applicable Domains. <p>i Important - Do not publish any changes in the Global Domain until you complete the upgrade to the next available version. This is necessary to avoid any potential issues caused by different policy revisions on the Global Domain and on other Domains.</p>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	<p>Install the latest version of the CPUSE from sk92449.</p> <p>Note - This is to make sure the CPUSE is able to support the required Upgrade Tools package.</p>
7	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
8	<p>In Management High Availability, before you start the upgrade on other servers:</p> <ol style="list-style-type: none"> Make sure the Primary Multi-Domain Server is upgraded and runs. Make sure the Multi-Domain Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794.

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

Procedure:

1. If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary

For instructions, see the [R81.20 Multi-Domain Security Management Administration Guide](#) - Chapter *Working with High Availability* - Section *Failure Recovery* - Subsection *Promoting the Secondary Multi-Domain Server to Primary*.

2. Make sure the Global Domain is Active on the Primary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the Primary Multi-Domain Server.
2	<p>From the left navigation panel, click Multi Domain > Domains. The table shows Domains and Multi-Domain Servers:</p> <ul style="list-style-type: none"> ▪ 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.
3	<p>In the leftmost column Domains, examine the bottom row Global for the Primary Multi-Domain Server. If the Global Domain is in the Standby state on the Primary Multi-Domain Server (marked with an empty "barrel" icon), then make it Active:</p> <ol style="list-style-type: none"> a. Right-click on the Primary Multi-Domain Server and click Connect to Domain Server. The High Availability Status window opens. b. In the section Connected To, click Actions > Set Active. c. Click Yes to confirm. d. Wait for the full synchronization to complete. e. Close SmartConsole.

3. Get the required Upgrade Tools on the Primary and on the Secondary Multi-Domain

Servers

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>

i 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.


Step	Instructions
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - 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"> Follow the instructions in the report. Run the Pre-Upgrade Verifier again.

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"> ■ If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> ■ If this Multi-Domain Server is not connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>

Step	Instructions
5	Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> Follow the instructions in the report. Run the Pre-Upgrade Verifier again.

6. On the Primary Multi-Domain Server, export the entire management database

Step	Instructions
1	Go to the <code>\$MDS_FWDIR/scripts/</code> directory: <pre>cd \$MDS_FWDIR/scripts</pre>
2	Export the management database: <ul style="list-style-type: none"> If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre>./migrate_server export -v R81.20 [-l -x] /<Full Path>/Primary_<Name of Exported File></pre> If this Multi-Domain Server is not connected to the Internet, run: <pre>./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Primary_<Name of Exported File></pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i> .
3	Calculate the MD5 for the exported database files: <pre>md5sum /<Full Path>/Primary_<Name of Database File>.tgz</pre>
4	Transfer the exported databases from the source Multi-Domain Server to an external storage: <pre>/<Full Path>/Primary_<Name of Database File>.tgz</pre> <p> Note - 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	Go to the <code>\$MDS_FWDIR/scripts/</code> directory: <pre>cd \$MDS_FWDIR/scripts</pre>
2	Export the management database: <ul style="list-style-type: none"> If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre>./migrate_server export -v R81.20 [-l -x] /<Full Path>/Secondary_<Name of Exported File></pre> If this Multi-Domain Server is not connected to the Internet, run: <pre>./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Secondary_<Name of Exported File></pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i> .
3	Calculate the MD5 for the exported database files: <pre>md5sum /<Full Path>/Secondary_<Name of Database File>.tgz</pre>
4	Transfer the exported databases from the source Multi-Domain Server to an external storage: <pre>/<Full Path>/Secondary_<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

8. Install the Primary R81.20 Multi-Domain Server

Step	Instructions
1	See the R81.20 Release Notes for requirements.

Step	Instructions
2	<ul style="list-style-type: none"> ■ 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"> • "Installing Software Packages on Gaia" on page 199. Select the R81.20 package and perform Upgrade. See sk92449 for detailed steps. • "Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 83. Do not perform initial configuration in SmartConsole. ■ If you upgrade from R80.20.M1 version, you must follow this procedure: <ul style="list-style-type: none"> • "Installing a Secondary Multi-Domain Server in Management High Availability" on page 85. Do not perform initial configuration in SmartConsole.


i **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 R81.20 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

i **Important** - See ["Upgrade Tools" on page 222](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 . Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See "Installing Software Packages on Gaia" on page 199 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 data-bbox="432 322 1460 421">cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre data-bbox="459 667 1460 853">[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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.
```

10. On the Primary R81.20 Multi-Domain Server, import the databases

Required JSON configuration file

If you installed the target R81.20 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.

i 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 Multi-Domain Log Servers, 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 Multi-Domain Log Servers, 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 R81.20 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 each server that migrates to a new IP address.</p> <p>Format for migrating only the Primary Multi-Domain Server to a new IP address</p> <pre data-bbox="475 427 1461 607">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</p> <pre data-bbox="475 730 1461 1070">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</p> <pre data-bbox="475 1193 1461 1659">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}, {"name": "<Name of Multi-Domain Log Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Multi-Domain Log Server>"}]</pre>

Step	Instructions
	<p>Example</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 migrate to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21 The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22 The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS The new IPv4 address of the target Primary R81.20 Multi-Domain Server is: 172.30.40.51 The new IPv4 address of the target Secondary R81.20 Multi-Domain Server is: 172.30.40.52 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> <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

-  **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line the Primary R81.20 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: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R81.20 Multi-Domain Server, to some directory.  Note - 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: <pre>md5sum /<Full Path>/Primary_<Name of Exported File>.tgz</pre>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory: <pre>cd \$MDS_FWDIR/scripts/</pre>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server is connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <pre data-bbox="628 360 1460 506">./migrate_server import -v R81.20 [-l -x] /<Full Path>/Primary_<Name of Exported File>.tgz</pre> • And at least one of the servers changed its IP address: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <pre data-bbox="708 636 1460 781">./migrate_server import -v R81.20 [-l -x] /<Full Path>/Primary_<Name of Exported File>.tgz</pre> ◦ Or run: <pre data-bbox="708 826 1460 1005">./migrate_server import -v R81.20 [-l -x] /var/log/mdss.json /<Full Path>/Primary_<Name of Exported File>.tgz</pre> ■ If this Multi-Domain Server is not connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <pre data-bbox="628 1099 1460 1279">./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Primary_<Name of Exported File>.tgz</pre> • And at least one of the servers changed its IP address: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <pre data-bbox="708 1413 1460 1592">./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /<Full Path>/Primary_<Name of Exported File>.tgz</pre> ◦ Or run: <pre data-bbox="708 1637 1460 1861">./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /var/log/mdss.json /<Full Path>/Primary_<Name of Exported File>.tgz</pre>

Step	Instructions
	<p>For details, see the R81.20 CLI Reference Guide - 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 CPCA) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="469 472 1460 535">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="469 663 1460 891">mdsstop_customer <IP Address or Name of Domain Management Server> mdsstart_customer <IP Address or Name of Domain Management Server> mdsstat</pre>

11. Install the Secondary R81.20 Multi-Domain Server

Step	Instructions
1	<p>See the R81.20 Release Notes for requirements.</p>
2	<ul style="list-style-type: none"> ■ 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"> • "Installing Software Packages on Gaia" on page 199. Select the R81.20 package and perform Upgrade. See sk92449 for detailed steps. • "Installing a Secondary Multi-Domain Server in Management High Availability" on page 85. Do not perform initial configuration in SmartConsole. ■ If you upgrade from R80.20.M1 version, you must follow this procedure: <ul style="list-style-type: none"> • "Installing a Secondary Multi-Domain Server in Management High Availability" on page 85. Do not perform initial configuration in SmartConsole.

- i 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 R81.20 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 R81.20 Multi-Domain Server

- i Note** - This step is needed only to be able to export the entire management database (for backup purposes) with the latest Upgrade Tools.
- i Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172.. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> </div> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre> </div>

- 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 R81.20 Multi-Domain Server, import the databases

Required JSON configuration file

If you installed the target R81.20 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 Multi-Domain Log Servers, 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 Multi-Domain Log Servers, 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 R81.20 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 each server that migrates to a new IP address.</p> <p>Format for migrating only the Primary Multi-Domain Server to a new IP address</p> <pre data-bbox="475 427 1460 607">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</p> <pre data-bbox="475 730 1460 1070">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</p> <pre data-bbox="475 1193 1460 1659">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}, {"name": "<Name of Multi-Domain Log Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Multi-Domain Log Server>"}]</pre>

Step	Instructions
	<p>Example</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 migrate to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21 The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22 The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS The new IPv4 address of the target Primary R81.20 Multi-Domain Server is: 172.30.40.51 The new IPv4 address of the target Secondary R81.20 Multi-Domain Server is: 172.30.40.52 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> <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

-  **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line the Secondary R81.20 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: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R81.20 Multi-Domain Server, to some directory.  Note - 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: <pre>md5sum /<Full Path>/Secondary_<Name of Exported File>.tgz</pre>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory: <pre>cd \$MDS_FWDIR/scripts/</pre>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server is connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <pre data-bbox="628 360 1460 506">./migrate_server import -v R81.20 [-l -x] /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> • And at least one of the servers changed its IP address: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <pre data-bbox="708 636 1460 781">./migrate_server import -v R81.20 [-l -x] /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> ◦ Or run: <pre data-bbox="708 826 1460 1005">./migrate_server import -v R81.20 [-l -x] /var/log/mdss.json /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> ■ If this Multi-Domain Server is not connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <pre data-bbox="628 1099 1460 1267">./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> • And at least one of the servers changed its IP address, run: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <pre data-bbox="708 1420 1460 1588">./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> ◦ Or run: <pre data-bbox="708 1644 1460 1856">./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /var/log/mdss.json /<Full Path>/Secondary_<Name of Exported File>.tgz</pre>

Step	Instructions
	For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i> .
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPCA) 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 <IP Address or Name of Domain Management Server> mdsstart_customer <IP Address or Name of Domain Management Server> mdsstat</pre>


14. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

15. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Primary Multi-Domain Server.
2	From the left navigation panel, click Multi-Domain > Domains .
3	From the top toolbar, open the Secondary Multi-Domain Server object.
4	From the left tree, click General .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

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:

- ["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 350](#)
- ["Upgrade of Security Management Servers and Log Servers" on page 224](#)


17. Reconfigure the User and Device Management Server

i Important - This step applies only if the User and Device Management (UDM) is configured on one of the Domain Management Servers.

Step	Instructions
1	Close all SmartConsole clients connected the R81.20 Multi-Domain Server.
2	Connect to the command line on the R81.20 Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.
5	Go to the main MDS context: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>mdsenv</pre> </div>
6	Examine the port numbers configured in the file <code>\$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</code> in the attribute " port () ": <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cat \$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</pre> </div> <p>Example:</p> <div style="border: 1px solid black; padding: 10px; margin-top: 5px;"> <pre>(: (My_Domain_Management_Server_1 :port (30000) :port_SL (30001) :ip_addr (192.168.2.1)) : (My_Domain_Management_Server_2 :port (30002) :port_SL (30003) :ip_addr (192.168.2.2)))</pre> </div>

Step	Instructions
7	<p>Configure the same port numbers in the file <code>\$UDMDIR/conf/cmas_list.conf</code> in the attribute "WSPort":</p> <pre>vi \$UDMDIR/conf/cmas_list.conf</pre> <p>Example:</p> <pre>192.168.2.1:WSPort=30000:MDSip=192.168.2.254 192.168.2.2:WSPort=30002:MDSip=192.168.2.254</pre>
8	Save the changes in the file and exit the editor.
9	<p>Restart the User and Device Management services:</p> <pre>udmstop ; udmstart</pre>

18. In SmartConsole of each applicable Domain Management Server, install policy on all SmartLSM Security Profiles

 **Important** - This step applies to each Domain Management Server that manages SmartLSM Security Profiles.

Step	Instructions
1	<p>Install the Access Control Policy:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	<p>Install the Threat Prevention Policy:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

19. Test the functionality on the Primary R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the Primary R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish the session.
4	<p>If there are Global Policies configured on the Global Domain:</p> <ul style="list-style-type: none"> a. Connect with SmartConsole to the Global Domain on your source Multi-Domain Server. b. Reassign all Global Policies to all applicable Domains. <p>Important - Do not publish any changes in the Global Domain until you complete the upgrade to the next available version. This is necessary to avoid any potential issues caused by different policy revisions on the Global Domain and on other Domains.</p>
5	You must close all GUI clients (SmartConsole applications) connected to the source Multi-Domain Server.
6	<p>Install the latest version of the CPUSE from sk92449.</p> <p>Note - This is to make sure the CPUSE is able to support the required Upgrade Tools package.</p>
7	Run the Pre-Upgrade Verifier on all source servers and fix all detected issues before you start the upgrade.
8	<p>In Management High Availability, before you start the upgrade on other servers:</p> <ul style="list-style-type: none"> a. Make sure the Primary Multi-Domain Server is upgraded and runs. b. Make sure the Multi-Domain Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794.

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

Procedure:

1. If the Primary Multi-Domain Server is not available, promote the Secondary Multi-Domain Server to be the Primary

For instructions, see the [R81.20 Multi-Domain Security Management Administration Guide](#) - Chapter *Working with High Availability* - Section *Failure Recovery* - Subsection *Promoting the Secondary Multi-Domain Server to Primary*.

2. Make sure the Global Domain is Active on the Primary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the Primary Multi-Domain Server.
2	<p>From the left navigation panel, click Multi Domain > Domains. The table shows Domains and Multi-Domain Servers:</p> <ul style="list-style-type: none"> ▪ 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.
3	<p>In the leftmost column Domains, examine the bottom row Global for the Primary Multi-Domain Server. If the Global Domain is in the Standby state on the Primary Multi-Domain Server (marked with an empty "barrel" icon), then make it Active:</p> <ol style="list-style-type: none"> a. Right-click on the Primary Multi-Domain Server and click Connect to Domain Server. The High Availability Status window opens. b. In the section Connected To, click Actions > Set Active. c. Click Yes to confirm. d. Wait for the full synchronization to complete. e. Close SmartConsole.

3. Get the required Upgrade Tools on the Primary and on the Secondary Multi-Domain

Servers

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPUpgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>

i 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.


Step	Instructions
3	Log in to the Expert mode.
4	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> If this Multi-Domain Server is not connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - 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"> Follow the instructions in the report. Run the Pre-Upgrade Verifier again.

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"> If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> If this Multi-Domain Server is not connected to the Internet, run: <pre>\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i>.</p>

Step	Instructions
5	Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> Follow the instructions in the report. Run the Pre-Upgrade Verifier again.

6. On the Primary Multi-Domain Server, export the entire management database

Step	Instructions
1	Go to the <code>\$MDS_FWDIR/scripts/</code> directory: <pre>cd \$MDS_FWDIR/scripts</pre>
2	Export the management database: <ul style="list-style-type: none"> If this Multi-Domain Server <i>is</i> connected to the Internet, run: <pre>./migrate_server export -v R81.20 [-l -x] /<Full Path>/Primary_<Name of Exported File></pre> If this Multi-Domain Server is not connected to the Internet, run: <pre>./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Primary_<Name of Exported File></pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i> .
3	Calculate the MD5 for the exported database files: <pre>md5sum /<Full Path>/Primary_<Name of Database File>.tgz</pre>
4	Transfer the exported databases from the source Multi-Domain Server to an external storage: <pre>/<Full Path>/Primary_<Name of Database File>.tgz</pre> <p> Note - 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"> <p>If this Multi-Domain Server <i>is</i> connected to the Internet, run:</p> <pre>./migrate_server export -v R81.20 [-l -x] /<Full Path>/Secondary_<Name of Exported File></pre> <p>If this Multi-Domain Server is not connected to the Internet, run:</p> <pre>./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Secondary_<Name of Exported File></pre> <p>For details, see the R81.20 CLI Reference Guide - 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 /<Full Path>/Secondary_<Name of Database File>.tgz</pre>
4	<p>Transfer the exported databases from the source Multi-Domain Server to an external storage:</p> <pre>/<Full Path>/Secondary_<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

8. Install another Primary R81.20 Multi-Domain Server

Step	Instructions
1	<p>See the R81.20 Release Notes for requirements.</p>
2	<p>Perform the clean install on another server in one of these ways:</p> <p>Important - Do not perform initial configuration in SmartConsole.</p> <ul style="list-style-type: none"> <p>Follow "Installing Software Packages on Gaia" on page 199. Select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.</p> <p>Follow "Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability" on page 83.</p>

i 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 R81.20 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

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> </div> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre> </div>

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.
```

10. On the Primary R81.20 Multi-Domain Server, import the databases

Required JSON configuration file

If you installed the target R81.20 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 Multi-Domain Log Servers, 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 Multi-Domain Log Servers, 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 R81.20 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 each server that migrates to a new IP address.</p> <p>Format for migrating only the Primary Multi-Domain Server to a new IP address</p> <pre data-bbox="475 427 1460 607">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</p> <pre data-bbox="475 730 1460 1070">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</p> <pre data-bbox="475 1193 1460 1659">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}, {"name": "<Name of Multi-Domain Log Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Multi-Domain Log Server>"}]</pre>

Step	Instructions
	<p>Example</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 migrate to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21 The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22 The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS The new IPv4 address of the target Primary R81.20 Multi-Domain Server is: 172.30.40.51 The new IPv4 address of the target Secondary R81.20 Multi-Domain Server is: 172.30.40.52 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> <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

-  **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line the Primary R81.20 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: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R81.20 Multi-Domain Server, to some directory.  Note - 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: <pre>md5sum /<Full Path>/Primary_<Name of Exported File>.tgz</pre>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory: <pre>cd \$MDS_FWDIR/scripts/</pre>

Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server is connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <div data-bbox="628 360 1460 506" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>./migrate_server import -v R81.20 [-l -x] /<Full Path>/Primary_<Name of Exported File>.tgz</pre> </div> • And at least one of the servers changed its IP address: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <div data-bbox="708 636 1460 781" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>./migrate_server import -v R81.20 [-l -x] /<Full Path>/Primary_<Name of Exported File>.tgz</pre> </div> ◦ Or run: <div data-bbox="708 826 1460 1005" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>./migrate_server import -v R81.20 [-l -x] /var/log/mdss.json /<Full Path>/Primary_<Name of Exported File>.tgz</pre> </div> ■ If this Multi-Domain Server is not connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <div data-bbox="628 1099 1460 1279" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Primary_<Name of Exported File>.tgz</pre> </div> • And at least one of the servers changed its IP address: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <div data-bbox="708 1413 1460 1592" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /<Full Path>/Primary_<Name of Exported File>.tgz</pre> </div> ◦ Or run: <div data-bbox="708 1641 1460 1861" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /var/log/mdss.json /<Full Path>/Primary_<Name of Exported File>.tgz</pre> </div>

Step	Instructions
	For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i> .
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPCA) 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 <IP Address or Name of Domain Management Server> mdsstart_customer <IP Address or Name of Domain Management Server> mdsstat</pre>

11. Install another Secondary R81.20 Multi-Domain Server

Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install on another server in one of these ways:</p> <p>Important - Do not perform initial configuration in SmartConsole.</p> <ul style="list-style-type: none"> Follow "Installing Software Packages on Gaia" on page 199. Select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. Follow "Installing a Secondary Multi-Domain Server in Management High Availability" on page 85.

i 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 R81.20 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 R81.20 Multi-Domain Server

i Note - This step is needed only to be able to export the entire management database (for backup purposes) with the latest Upgrade Tools.

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.</p> <p>Run this command in the Expert mode:</p> <pre> cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre>

i 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 R81.20 Multi-Domain Server, import the databases

Required JSON configuration file

If you installed the target R81.20 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 Multi-Domain Log Servers, 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 Multi-Domain Log Servers, 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 R81.20 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 each server that migrates to a new IP address.</p> <p>Format for migrating only the Primary Multi-Domain Server to a new IP address</p> <pre data-bbox="475 427 1460 607">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers to new IP addresses</p> <pre data-bbox="475 730 1460 1070">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}]</pre> <p>Format for migrating both the Primary and the Secondary Multi-Domain Servers, and the Multi-Domain Log Server to new IP addresses</p> <pre data-bbox="475 1193 1460 1659">[{"name": "<Name of Primary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Primary R81.20 Multi-Domain Server>"}, {"name": "<Name of Secondary Multi-Domain Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of Secondary R81.20 Multi-Domain Server>"}, {"name": "<Name of Multi-Domain Log Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Multi-Domain Log Server>"}]</pre>

Step	Instructions
	<p>Example</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 migrate to new IP addresses. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source Primary R80.30 Multi-Domain Server is: 192.168.10.21 The current IPv4 address of the source Secondary R80.30 Multi-Domain Server is: 192.168.10.22 The name of the source Primary R80.30 Multi-Domain Server object in SmartConsole is: MyPrimaryMDS The name of the source Secondary R80.30 Multi-Domain Server object in SmartConsole is: MySecondaryMDS The new IPv4 address of the target Primary R81.20 Multi-Domain Server is: 172.30.40.51 The new IPv4 address of the target Secondary R81.20 Multi-Domain Server is: 172.30.40.52 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> <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

-  **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line the Secondary R81.20 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: <pre>cplic print</pre> If it is not already installed, then install a valid license now.
5	Transfer the exported database from an external storage to the R81.20 Multi-Domain Server, to some directory.  Note - 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: <pre>md5sum /<Full Path>/Secondary_<Name of Exported File>.tgz</pre>
7	Go to the <code>\$MDS_FWDIR/scripts/</code> directory: <pre>cd \$MDS_FWDIR/scripts/</pre>


Step	Instructions
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Server is connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <pre data-bbox="628 360 1460 506">./migrate_server import -v R81.20 [-l -x] /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> • And at least one of the servers changed its IP address: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <pre data-bbox="708 636 1460 781">./migrate_server import -v R81.20 [-l -x] /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> ◦ Or run: <pre data-bbox="708 826 1460 1005">./migrate_server import -v R81.20 [-l -x] /var/log/mdss.json /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> ■ If this Multi-Domain Server is not connected to the Internet: <ul style="list-style-type: none"> • And none of the servers changed their IP addresses, run: <pre data-bbox="628 1099 1460 1279">./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> • And at least one of the servers changed its IP address, run: <ul style="list-style-type: none"> ◦ Make sure the required file <code>/var/log/mdss.json</code> exists and run: <pre data-bbox="708 1417 1460 1597">./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /<Full Path>/Secondary_<Name of Exported File>.tgz</pre> ◦ Or run: <pre data-bbox="708 1641 1460 1861">./migrate_server import -v R81.20 [-l -x] -skip_upgrade_tools_check /var/log/mdss.json /<Full Path>/Secondary_<Name of Exported File>.tgz</pre>

Step	Instructions
	For details, see the R81.20 CLI Reference Guide - Chapter <i>Multi-Domain Security Management Commands</i> - Section <i>migrate_server</i> .
9	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPCA) 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 <IP Address or Name of Domain Management Server> mdsstart_customer <IP Address or Name of Domain Management Server> mdsstat</pre>

14. Update the object version of the Secondary Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Primary Multi-Domain Server.
2	From the left navigation panel, click Multi-Domain > Domains .
3	From the top toolbar, open the Secondary Multi-Domain Server object.
4	From the left tree, click General .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

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:

- ["Upgrading a Multi-Domain Log Server from R80.20 and higher" on page 350](#)
- ["Upgrade of Security Management Servers and Log Servers" on page 224](#)


16. Reconfigure the User and Device Management Server

i Important - This step applies only if the User and Device Management (UDM) is configured on one of the Domain Management Servers.

Step	Instructions
1	Close all SmartConsole clients connected the R81.20 Multi-Domain Server.
2	Connect to the command line on the R81.20 Multi-Domain Server.
3	Log in with the superuser credentials.
4	Log in to the Expert mode.
5	Go to the main MDS context: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>mdsenv</pre> </div>
6	Examine the port numbers configured in the file <code>\$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</code> in the attribute "port ()" : <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>cat \$MDSDIR/conf/mdsdb/webservices_cmas_ports.conf</pre> </div> Example: <div style="border: 1px solid black; padding: 10px; margin-top: 5px;"> <pre>(: (My_Domain_Management_Server_1 :port (30000) :port_SL (30001) :ip_addr (192.168.2.1)) : (My_Domain_Management_Server_2 :port (30002) :port_SL (30003) :ip_addr (192.168.2.2)))</pre> </div>

Step	Instructions
7	<p>Configure the same port numbers in the file <code>\$UDMDIR/conf/cmas_list.conf</code> in the attribute "WSPort":</p> <pre>vi \$UDMDIR/conf/cmas_list.conf</pre> <p>Example:</p> <pre>192.168.2.1:WSPort=30000:MDSip=192.168.2.254 192.168.2.2:WSPort=30002:MDSip=192.168.2.254</pre>
8	Save the changes in the file and exit the editor.
9	<p>Restart the User and Device Management services:</p> <pre>udmstop ; udmstart</pre>

17. In SmartConsole of each applicable Domain Management Server, install policy on all SmartLSM Security Profiles

 **Important** - This step applies to each Domain Management Server that manages SmartLSM Security Profiles.

Step	Instructions
1	<p>Install the Access Control Policy:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Access Control Policy must install successfully.
2	<p>Install the Threat Prevention Policy:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Select the applicable SmartLSM Security Profile objects. Click Install. The Threat Prevention Policy must install successfully.

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

18. Test the functionality on the Primary R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the Primary R81.20 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 R80.20 and higher

This section provides instructions to upgrade a Multi-Domain Log Server from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions:

- *["Upgrading a Multi-Domain Log Server from R80.20 and higher with CPUSE" on page 351](#)*
- *["Upgrading a Multi-Domain Log Server from R80.20 and higher with Advanced upgrade" on page 356](#)*
- *["Upgrading a Multi-Domain Log Server from R80.20 and higher with Migration" on page 363](#)*

For additional information related to these upgrade procedures, see [sk163814](#).

For configuration information, see the [R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
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**

- i Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 . Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>

- i 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. Create the required JSON configuration file on the Multi-Domain Log Server

i 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.
Skip this step.
- Even if only one of the servers migrates to a new IP address, all the other servers (including all Multi-Domain Log Servers, Log Servers, and SmartEvent Servers) must get this configuration file.
You must use the same JSON configuration file on all servers (including the Secondary Multi-Domain Servers, Multi-Domain Log Servers, 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 Multi-Domain Log Server Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address. Format for migrating a Multi-Domain Server / Log Server / SmartEvent Server to a new IP address:</p> <pre>[{"name": "<Name of Server #1 Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Server #1>"}, {"name": "<Name of Server #2 Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Server #2>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Multi-Domain Security Management environment - the Multi-Domain Server and the Multi-Domain Log Server. The Multi-Domain Server migrates to a new IP address. The Multi-Domain Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Multi-Domain Server is: 192.168.10.21 The name of the source R80.30 Multi-Domain Server object in SmartConsole is: MyMultiDomainServer The new IPv4 address of the target R81.20 Multi-Domain Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Multi-Domain Server and on the Multi-Domain Log Server: [{"name": "MyMultiDomainServer", "newIpAddress4": "172.30.40.51"}] <p> Important - All servers in this environment must get the same configuration file.</p>

3. Upgrade the Multi-Domain Log Server with CPUSE

See ["Installing Software Packages on Gaia" on page 199](#) and follow the applicable action plan.

4. Update the version of the Multi-Domain Log Server object

Step	Instructions
1	Connect with SmartConsole to the R81.20 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click Multi-Domain > Domains .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click General .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

5. Test the functionality on the R81.20 Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

6. Test the functionality on the R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
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

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 and follow the applicable action plan for the <i>Local - Offline</i> installation.</p>
3	<p>Make sure the package is installed.</p> <p>Run this command in the Expert mode:</p> <pre> cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre>

i 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"> ▪ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 539 1461 640">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> ▪ If this Multi-Domain Log Server is not connected to the Internet, run: <pre data-bbox="512 696 1461 797">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - 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"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
6	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre data-bbox="432 1155 1461 1223">cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> ▪ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1346 1461 1447">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ▪ If this Multi-Domain Log Server is not connected to the Internet, run: <pre data-bbox="512 1503 1461 1626">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> <p>For details, see the R81.20 CLI Reference Guide - 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 data-bbox="432 1805 1461 1872">md5sum /<Full Path>/<Name of Database File>.tgz</pre>

Step	Instructions
9	<p>Transfer the exported databases from the source Multi-Domain Log Server to an external storage:</p> <pre style="border: 1px solid black; padding: 5px; margin: 10px 0;">/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install a new R81.20 Multi-Domain Log Server

Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install in one of these ways (do not perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing a Multi-Domain Log Server" on page 88.

4. Get the required Upgrade Tools on the R81.20 server

 **Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 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-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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 R81.20 Multi-Domain Log Server, import the databases

Step	Instructions
1	Connect to the command line on the R81.20 Multi-Domain Log 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> <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 R81.20 Multi-Domain Log Server, to some directory.</p> <p>Note - Make sure to transfer the file in the binary mode.</p>

Step	Instructions
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 data-bbox="432 360 1458 427">md5sum /<Full Path>/<Name of Exported File>.tgz</pre>
7	<p>Go to the \$MDS_FWDIR/scripts/ directory:</p> <pre data-bbox="432 506 1458 573">cd \$MDS_FWDIR/scripts/</pre>
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 689 1458 790">./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ■ If this Multi-Domain Log Server is not connected to the Internet, run: <pre data-bbox="512 846 1458 981">./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>For details, see the R81.20 CLI Reference Guide - 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="432 1144 1458 1211">mdsstat</pre> <ul style="list-style-type: none"> ■ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd". ■ The state of the CPCA daemon must be "N/R" on the MDS level. ■ The state of the CPCA daemon must be "down" on the Domain Log Server level. <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="432 1585 1458 1809">mdsstop_customer <IP Address or Name of Domain Log Server> mdsstart_customer <IP Address or Name of Domain Log Server> mdsstat</pre>

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Update the version of the Multi-Domain Log Server object

Step	Instructions
1	Connect with SmartConsole to the R81.20 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click Multi-Domain > Domains .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click General .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

8. Test the functionality on the R81.20 Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

9. Test the functionality on the R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
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**

- i Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 . Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1 </pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre>

- i 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"> ▪ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 539 1458 640">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20</pre> ▪ If this Multi-Domain Log Server is not connected to the Internet, run: <pre data-bbox="512 696 1458 797">\$MDS_FWDIR/scripts/migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - 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"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
6	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre data-bbox="432 1155 1458 1223">cd \$MDS_FWDIR/scripts</pre>
7	<p>Export the management database:</p> <ul style="list-style-type: none"> ▪ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1346 1458 1447">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ▪ If this Multi-Domain Log Server is not connected to the Internet, run: <pre data-bbox="512 1503 1458 1626">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> <p>For details, see the R81.20 CLI Reference Guide - 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 data-bbox="432 1794 1458 1861">md5sum /<Full Path>/<Name of Database File>.tgz</pre>


Step	Instructions
9	<p>Transfer the exported databases from the source Multi-Domain Log Server to an external storage:</p> <pre style="border: 1px solid black; padding: 5px; margin: 10px 0;">/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install another R81.20 Multi-Domain Log Server

Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install on another server in one of these ways (do not perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing a Multi-Domain Log Server" on page 88.

 **Important** - The IP addresses of the source and target R81.20 servers **must be the same**. If it is necessary to have a different IP address on the R81.20 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 541](#).

4. Get the required Upgrade Tools on the R81.20 server

 **Important** - See ["Upgrade Tools" on page 222](#) to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	<p>Download the R81.20 Upgrade Tools from the sk135172..</p> <p>Note - This is a CPUSE Offline package.</p>
2	<p>Install the R81.20 Upgrade Tools with CPUSE.</p> <p>See "Installing Software Packages on Gaia" on page 199 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-R81.20 BuildNumber 1 </pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre>

i 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 R81.20 Multi-Domain Log Server, import the databases

Step	Instructions
1	Connect to the command line on the R81.20 Multi-Domain Log 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> <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 R81.20 Multi-Domain Log Server, to some directory.</p> <p>i Note - Make sure to transfer the file in the binary mode.</p>

Step	Instructions
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 data-bbox="432 360 1458 423">md5sum /<Full Path>/<Name of Exported File>.tgz</pre>
7	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre data-bbox="432 506 1458 568">cd \$MDS_FWDIR/scripts/</pre>
8	<p>Import the management database:</p> <ul style="list-style-type: none"> ▪ If this Multi-Domain Log Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 689 1458 792">./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ▪ If this Multi-Domain Log Server is not connected to the Internet, run: <pre data-bbox="512 846 1458 981">./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>For details, see the R81.20 CLI Reference Guide - 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="432 1144 1458 1207">mdsstat</pre> <ul style="list-style-type: none"> ▪ The state of the FWM, FWD, and CPD daemons must be "up" on all levels. These daemons must show their PID, or "pnd". ▪ The state of the CPCA daemon must be "N/R" on the MDS level. ▪ The state of the CPCA daemon must be "down" on the Domain Log Server level. <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="432 1585 1458 1809">mdsstop_customer <IP Address or Name of Domain Log Server> mdsstart_customer <IP Address or Name of Domain Log Server> mdsstat</pre>

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Update the version of the Multi-Domain Log Server object

Step	Instructions
1	Connect with SmartConsole to the R81.20 Multi-Domain Server that manages the Multi-Domain Log Server.
2	From the left navigation panel, click Multi-Domain > Domains .
3	From the top toolbar, open the Multi-Domain Log Server object.
4	From the left tree, click General .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

8. Test the functionality on the R81.20 Multi-Domain Log Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Multi-Domain Log Server.
2	Make sure the management database and configuration were upgraded correctly.

9. Test the functionality on the R81.20 Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Multi-Domain Server that manages the Multi-Domain Log Server.
2	Make sure the logging works as expected.

10. Disconnect the old Multi-Domain Log Server from the network

Disconnect the network cables the old Multi-Domain Log Server.

11. 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 Security Management Servers and dedicated Log Servers from R80.20.M1, R80.20, R80.20.M2, R80.30, or higher versions:

- *"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE" on page 371*
- *"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade" on page 377*
- *"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration" on page 388*
- *"Upgrading Endpoint Security Management Servers in Management High Availability from R80.20 and higher" on page 399*

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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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**

- i Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 . Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> <p>The output must show the same build number you see in the name of the downloaded TGZ package.</p> <p>Example</p> <p>Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz</p> <pre>[Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]#</pre>

- i 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. Create the required JSON configuration file

Important:

- If none of the servers in the same Endpoint Security Management Server environment changed their original IP addresses, then you do **not** need to create the special JSON configuration file. Skip this step.
- 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.
You must use the same JSON configuration file on all servers (including Log Servers and SmartEvent Servers) in the same Endpoint Security Management Server environment.

To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the Endpoint Security Management Server / Endpoint Policy Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address. Format for migrating a single Log Server / SmartEvent Server to a new IP address:</p> <pre>[{"name": "<Name of Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Server>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Endpoint Security Management Server environment - the Endpoint Security Management Server and the Log Server. The Endpoint Security Management Server remains with the original IP address. The Log Server migrates to a new IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Log Server is: 192.168.10.21 The name of the source R80.30 Log Server object in SmartConsole is: MyLogServer The new IPv4 address of the target R81.20 Log Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Endpoint Security Management Server and on the Log Server: <pre>[{"name": "MyLogServer", "newIpAddress4": "172.30.40.51"}]</pre> <p> Important - All servers in this environment must get the same configuration file.</p>

3. Upgrade the Endpoint Security Management Server or Endpoint Policy Server with CPUSE


See ["Installing Software Packages on Gaia" on page 199](#) and follow the applicable action plan.

4. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

5. Upgrade the dedicated Endpoint Policy Servers

This step is part of the upgrade procedure of an Endpoint Security Management 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.

See ["Upgrade of Endpoint Security Management Servers and Endpoint Policy Servers" on page 370](#).

6. Update the object version of the dedicated Endpoint Policy Servers

i 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 R81.20 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click General Properties .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

7. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R81.20 Endpoint Security Management Server.
2	In the top left corner, click Menu > Install database .
3	Select all objects.
4	Click Install .
5	Click OK .

8. Install the Event Policy

i Important - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R81.20 Endpoint Server.

Step	Instructions
1	Connect with the SmartConsole to the R81.20 Endpoint Server.
2	In the SmartConsole, from the left navigation panel, click Logs & Monitor .
3	At the top, click + to open a new tab.

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

9. Test the functionality on the R81.20 Endpoint Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Endpoint Security Management Server. Make sure the management database and configuration were upgraded correctly.
2	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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: <div data-bbox="432 869 1458 974" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> </div> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <div data-bbox="432 1211 1458 1402" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre> </div>


i 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 <code>\$FWDIR/scripts/</code> directory:</p> <pre data-bbox="432 427 1458 488">cd \$FWDIR/scripts</pre>
3	<p>Run the Pre-Upgrade Verifier.</p> <ul style="list-style-type: none"> ▪ If this Endpoint Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 611 1458 672">./migrate_server verify -v R81.20</pre> ▪ If this Endpoint Server is not connected to the Internet, run: <pre data-bbox="512 723 1458 824">./migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> <p>For details, see the R81.20 CLI Reference Guide - 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"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
4	<p>Export the management database:</p> <ul style="list-style-type: none"> ▪ If this Endpoint Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1234 1458 1335">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ▪ If this Endpoint Server is not connected to the Internet, run: <pre data-bbox="512 1386 1458 1520">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> <p> Notes:</p> <ul style="list-style-type: none"> ▪ You can also export the MSI packages with the "<code>--include-uepm-msi-files</code>" option. ▪ For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.
7	<p>Calculate the MD5 for the exported database files:</p> <pre data-bbox="432 1854 1458 1915">md5sum /<Full Path>/<Name of Database File>.tgz</pre>


Step	Instructions
8	<p>Transfer the exported databases from the source Endpoint Server to an external storage:</p> <pre style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install a new R81.20 Endpoint Security Management Server or Endpoint Policy Server


Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install in one of these ways (do not perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing an Endpoint Security Management Server" on page 91. ▪ Follow "Installing an Endpoint Policy Server" on page 96.

-  **Important** - These options are available:
- The IP addresses of the source and target servers **can be the same**. If in the future it is necessary to have a different IP address on the R81.20 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 servers **can be different**. you must create a special JSON configuration file `mdss.json` that contains **each** server that migrates to a new IP address. 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 R81.20 server

-  **Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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 R81.20 Endpoint Security Management Server or Endpoint Policy Server, import the databases

Required JSON configuration file

If you installed the target R81.20 Endpoint Server with a different IP address than the source Endpoint Server, you must create a special JSON configuration file before you import the management database from the source Endpoint Server. Note that you have to issue licenses for the new IP address.


i Important:

- If none of the servers in the same Endpoint Security 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 Endpoint Security environment.


To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R81.20 Endpoint Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address.</p> <p>Format for migrating a single Endpoint Server to a new IP address:</p> <pre>[{"name": "<Name of Endpoint Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Endpoint Server>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Endpoint Security environment - the Endpoint Security Management Server and the Log Server. The Endpoint Security Management Server migrates to a new IP address. The Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Endpoint Security Management Server is: 192.168.10.21 The name of the source R80.30 Endpoint Security Management Server object in SmartConsole is: MyEndpointMgmtServer The new IPv4 address of the target R81.20 Endpoint Security Management Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Endpoint Security Management Server and on the Log Server: <pre>[{"name": "MyEndpointMgmtServer", "newIpAddress4": "172.30.40.51"}]</pre> <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

-  **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line on the R81.20 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 R81.20 Endpoint Server, to some directory.</p> <p> Note - 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 Endpoint Server:</p> <pre>md5sum /<Full Path>/<Name of Database File>.tgz</pre>
6	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre>cd \$FWDIR/scripts/</pre>
7	<p>Import the management database:</p> <ul style="list-style-type: none"> ▪ If this Endpoint Server <i>is</i> connected to the Internet, run: <pre>./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ▪ If this Endpoint Server is not connected to the Internet, run: <pre>./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>i Notes:</p> <ul style="list-style-type: none"> ▪ The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands). ▪ You can also import the MSI packages with the "--include-uepm-msi-files" option. ▪ For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Install the new licenses

i **Important** - This step applies only if the target R81.20 Endpoint Server has a different IP address than the source Endpoint Server.

Step	Instructions
1	Issue licenses for the new IP address in your Check Point User Center count.

Step	Instructions
2	Install the new licenses on the R81.20 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 an Endpoint Security Management Server. If you upgrade a dedicated Endpoint Policy Server, then skip this step.

i 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.

See ["Upgrade of Endpoint Security Management Servers and Endpoint Policy Servers" on page 370](#).

9. Update the object version of the dedicated Endpoint Policy Servers


i 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 R81.20 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click General Properties .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R81.20 Endpoint Security Management Server.
2	In the top left corner, click Menu > Install database .
3	Select all objects.
4	Click Install .
5	Click OK .

11. Install the Event Policy

 **Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R81.20 Endpoint Server.

Step	Instructions
1	Connect with the SmartConsole to the R81.20 Endpoint Server.
2	In the SmartConsole, from the left navigation panel, click Logs & Monitor .
3	At the top, click + to open a new tab.
4	In the bottom left corner, in the External Apps section, click SmartEvent Settings & Policy . The Legacy SmartEvent client opens.
5	In the top left corner, click Menu > Actions > Install Event Policy .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click Close .
9	Close the Legacy SmartEvent client.

12. Test the functionality on the R81.20 Endpoint Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Endpoint Security Management Server. Make sure the management database and configuration were upgraded correctly.
2	Connect with SmartConsole to the R81.20 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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

i Important - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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: <div data-bbox="432 871 1458 972" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 </pre> </div> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <div data-bbox="432 1211 1458 1400" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre> [Expert@HostName:0]# cpprod_util CPPROD_GetValue CPupgrade-tools-R81.20 BuildNumber 1 993000222 [Expert@HostName:0]# </pre> </div>

i 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	Go to the <code>\$FWDIR/scripts/</code> directory: <pre data-bbox="432 427 1458 488">cd \$FWDIR/scripts</pre>
3	Run the Pre-Upgrade Verifier. <ul style="list-style-type: none"> ▪ If this Endpoint Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 611 1458 672">./migrate_server verify -v R81.20</pre> ▪ If this Endpoint Server is not connected to the Internet, run: <pre data-bbox="512 723 1458 824">./migrate_server verify -v R81.20 -skip_upgrade_tools_check</pre> For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i> .
4	Read the Pre-Upgrade Verifier output. If it is necessary to fix errors: <ol style="list-style-type: none"> a. Follow the instructions in the report. b. Run the Pre-Upgrade Verifier again.
4	Export the management database: <ul style="list-style-type: none"> ▪ If this Endpoint Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 1234 1458 1335">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ▪ If this Endpoint Server is not connected to the Internet, run: <pre data-bbox="512 1386 1458 1520">./migrate_server export -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> <p>i Notes:</p> <ul style="list-style-type: none"> ▪ You can also export the MSI packages with the "<code>--include-uepm-msi-files</code>" option. ▪ For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.
7	Calculate the MD5 for the exported database files: <pre data-bbox="432 1854 1458 1915">md5sum /<Full Path>/<Name of Database File>.tgz</pre>


Step	Instructions
8	<p>Transfer the exported databases from the source Endpoint Server to an external storage:</p> <pre style="border: 1px solid gray; padding: 5px; margin: 10px 0;">/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

3. Install a new R81.20 Endpoint Security Management Server or Endpoint Policy Server


Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	<p>Perform the clean install in one of these ways (do not perform initial configuration in SmartConsole):</p> <ul style="list-style-type: none"> ▪ Follow "Installing Software Packages on Gaia" on page 199 - select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. ▪ Follow "Installing an Endpoint Security Management Server" on page 91. ▪ Follow "Installing an Endpoint Policy Server" on page 96.

-  **Important** - These options are available:
- The IP addresses of the source and target servers **can be the same**. If in the future it is necessary to have a different IP address on the R81.20 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 servers **can be different**. you must create a special JSON configuration file `mdss.json` that contains **each** server that migrates to a new IP address. 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 R81.20 server

-  **Important** - See "[Upgrade Tools](#)" on page 222 to understand if your server can download and install the latest version of the Upgrade Tools automatically.

Step	Instructions
1	Download the R81.20 Upgrade Tools from the sk135172 .. Note - This is a CPUSE Offline package.
2	Install the R81.20 Upgrade Tools with CPUSE. See " Installing Software Packages on Gaia " on page 199 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-R81.20 BuildNumber 1</pre> The output must show the same build number you see in the name of the downloaded TGZ package. Example Name of the downloaded package: ngm_upgrade_wrapper_993000222_1.tgz <pre>[Expert@HostName:0]# cprod_util CPPROD_GetValue CPupgrade-tools-R81.20 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 R81.20 Endpoint Security Management Server or Endpoint Policy Server, import the databases

Required JSON configuration file

If you installed the target R81.20 Endpoint Server with a different IP address than the source Endpoint Server, you must create a special JSON configuration file before you import the management database from the source Endpoint Server. Note that you have to issue licenses for the new IP address.


i Important:

- If none of the servers in the same Endpoint Security 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 Endpoint Security environment.


To create the required JSON configuration file:

Step	Instructions
1	Connect to the command line on the target R81.20 Endpoint Server.
2	Log in to the Expert mode.
3	<p>Create the <code>/var/log/mdss.json</code> file that contains each server that migrates to a new IP address.</p> <p>Format for migrating a single Endpoint Server to a new IP address:</p> <pre>[{"name": "<Name of Endpoint Server Object in SmartConsole>", "newIpAddress4": "<New IPv4 Address of R81.20 Endpoint Server>"}]</pre>

Step	Instructions
	<p>Example</p> <p>There are 2 servers in the R80.30 Endpoint Security environment - the Endpoint Security Management Server and the Log Server. The Endpoint Security Management Server migrates to a new IP address. The Log Server remains with the original IP address.</p> <ol style="list-style-type: none"> The current IPv4 address of the source R80.30 Endpoint Security Management Server is: 192.168.10.21 The name of the source R80.30 Endpoint Security Management Server object in SmartConsole is: MyEndpointMgmtServer The new IPv4 address of the target R81.20 Endpoint Security Management Server is: 172.30.40.51 The required syntax for the JSON configuration file you must use on the Endpoint Security Management Server and on the Log Server: <pre>[{"name": "MyEndpointMgmtServer", "newIpAddress4": "172.30.40.51"}]</pre> <p> Important - All servers in this environment must get the same configuration file.</p>

Importing the databases

 **Important** - Make sure you followed the instructions in the above section "Required JSON configuration file".

Step	Instructions
1	Connect to the command line on the R81.20 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 R81.20 Endpoint Server, to some directory.</p> <p> Note - 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 Endpoint Server:</p> <pre>md5sum /<Full Path>/<Name of Database File>.tgz</pre>
6	<p>Go to the \$FWDIR/scripts/ directory:</p> <pre>cd \$FWDIR/scripts/</pre>
7	<p>Import the management database:</p> <ul style="list-style-type: none"> ▪ If this Endpoint Server <i>is</i> connected to the Internet, run: <pre>./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ▪ If this Endpoint Server is not connected to the Internet, run: <pre>./migrate_server import -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>i Notes:</p> <ul style="list-style-type: none"> ▪ The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands). ▪ You can also import the MSI packages with the "--include-uepm-msi-files" option. ▪ For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.

6. Install the R81.20 SmartConsole

See ["Installing SmartConsole" on page 106](#).

7. Install the new licenses

i **Important** - This step applies only if the target R81.20 Endpoint Server has a different IP address than the source Endpoint Server.

Step	Instructions
1	Issue licenses for the new IP address in your Check Point User Center count.

Step	Instructions
2	Install the new licenses on the R81.20 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 an Endpoint Security Management 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.

See ["Upgrade of Endpoint Security Management Servers and Endpoint Policy Servers" on page 370](#).

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 R81.20 Security Management Server that manages the Endpoint Policy Server.
2	From the left navigation panel, click Gateways & Servers .
3	Open the object of the Endpoint Policy Server.
4	From the left tree, click General Properties .
5	In the Platform section > in the Version field, select R81.20 .
6	Click OK .

10. Install the management database

Step	Instructions
1	Connect with SmartConsole to the R81.20 Endpoint Security Management Server.
2	In the top left corner, click Menu > Install database .
3	Select all objects.
4	Click Install .
5	Click OK .

11. Install the Event Policy

 **Important** - This step applies only if the **SmartEvent Correlation Unit** Software Blade is enabled on the R81.20 Endpoint Server.

Step	Instructions
1	Connect with the SmartConsole to the R81.20 Endpoint Server.
2	In the SmartConsole, from the left navigation panel, click Logs & Monitor .
3	At the top, click + to open a new tab.
4	In the bottom left corner, in the External Apps section, click SmartEvent Settings & Policy . The Legacy SmartEvent client opens.
5	In the top left corner, click Menu > Actions > Install Event Policy .
6	Confirm.
7	Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded
8	Click Close .
9	Close the Legacy SmartEvent client.

12. Test the functionality on the R81.20 Endpoint Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 Endpoint Security Management Server. Make sure the management database and configuration were upgraded correctly.
2	Connect with SmartConsole to the R81.20 Endpoint Policy Server. Make sure the everything works correctly.

13. Disconnect the old Endpoint Server from the network

Disconnect the cables from the old Endpoint Server.

14. 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, R80.30, or higher versions.
- 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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Only the latest published database revision is upgraded. If there are pending changes, we recommend to Publish 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 sk92449 . Note - 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 Primary Endpoint Security Management Server with one of the supported methods.</p> <ul style="list-style-type: none"> ▪ CPUSE See <i>"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE" on page 371</i> ▪ Advanced Upgrade See <i>"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade" on page 377</i> ▪ Migration See <i>"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration" on page 388</i>
2	<p>Upgrade the Secondary Endpoint Security Management Server with one of the supported methods.</p> <p> Important - Make sure the Endpoint Security Management Servers can communicate with each other and SIC works between these servers. For details, see sk179794.</p> <ul style="list-style-type: none"> ▪ CPUSE See <i>"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with CPUSE" on page 371</i> ▪ Advanced Upgrade See <i>"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Advanced Upgrade" on page 377</i> ▪ Migration See <i>"Upgrading an Endpoint Security Management Server or Endpoint Policy Server from R80.20 and higher with Migration" on page 388</i>
3	<p>Get the R81.20 SmartConsole. See <i>"Installing SmartConsole" on page 106</i>.</p>
4	<p>Connect with SmartConsole to the R81.20 Primary Endpoint Security Management Server.</p>

Step	Instructions
5	<p>Update the object version of the Secondary Endpoint Security Management Server:</p> <ol style="list-style-type: none"> From the left navigation panel, click Gateways & Servers. Open the Secondary Endpoint Security Management Server object. From the left tree, click General Properties. In the Platform section > in the Version field, select R81.20. Click OK.
6	<p>Make sure Secure Internal Communication (SIC) works correctly with the Secondary Security Management Server:</p> <ol style="list-style-type: none"> From the left navigation panel, click Gateways & Servers. Open the Secondary Security Management Server object. On the General Properties page, click Communication. Click Test SIC Status. The SIC Status must show Communicating. Click Close. Click OK.
7	<p>Install the management database:</p> <ol style="list-style-type: none"> In the top left corner, click Menu > Install database. Select all objects. Click Install. Click OK.
8	<p>Install the Event Policy.</p> <p> Important - This step applies only if the SmartEvent Correlation Unit Software Blade is enabled on the R81.20 Endpoint Security Management Server.</p> <ol style="list-style-type: none"> In the SmartConsole, from the left navigation panel, click Logs & Monitor. At the top, click + to open a new tab. In the bottom left corner, in the External Apps section, click SmartEvent Settings & Policy. The Legacy SmartEvent client opens. In the top left corner, click Menu > Actions > Install Event Policy. Confirm. Wait for these messages to appear: SmartEvent Policy Installer installation complete SmartEvent Policy Installer installation succeeded Click Close. Close the Legacy SmartEvent client.

Step	Instructions
9	<p>Synchronize the Endpoint Security Management Servers:</p> <ol style="list-style-type: none">In the top left corner, click Menu > Management High Availability.In the Peers section, click Actions > Sync Peer.The status must show Successfully synced for all peers.

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 404](#)
- ["Upgrading ClusterXL, VSX Cluster, or VRRP Cluster" on page 417](#)
- ["Full High Availability Cluster on Check Point Appliances" on page 180](#)

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 405](#)
 - ["Upgrading a VSX Gateway with CPUSE" on page 409](#)
- ★ **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

Upgrading a Security Gateway with CPUSE

 **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

 **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 "Backing Up and Restoring" on page 17).
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Upgrade the Management Server and Log Servers.
4	Upgrade the licenses on the Security Gateway, if needed. See "Working with Licenses" on page 680 .
4	<p>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</p> <p>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.</p> <p>As a result, different issues can occur in the upgraded Security Gateway.</p>

Procedure:

1. On the Security Gateway, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

i Important - You must reboot the Security Gateway after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	See "Installing Software Packages on Gaia" on page 199 . Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Upgrade . See sk92449 for detailed steps.
Clean Install of R81.20 with CPUSE	See "Installing Software Packages on Gaia" on page 199 . Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install . See sk92449 for detailed steps.
Clean Install of R81.20 from scratch	Follow "Installing a Security Gateway" on page 110 - only the step "Install the Security Gateway" . i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Security Gateway (prior to the upgrade).

2. In SmartConsole, establish SIC with the Security Gateway

i Important - This step is required only if you performed a Clean Install of R81.20 on this Security Gateway.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click Gateways & Servers .
3	Open the Security Gateway object.
4	From the left tree, click General Properties .

Step	Instructions
5	Click the Communication button.
6	Click Reset .
7	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Security Gateway.
8	In the Confirm one-time password field, enter the same Activation Key again.
9	Click Initialize .
10	The Trust state field must show Trust established .
11	Click Close to close the Communication window.
12	Click OK to close the Security Gateway Properties 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 R81.20 Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click Gateways & Servers .
3	Open the Security Gateway object.
4	From the left tree, click the General Properties page.
5	In the Platform section > Version field, select R81.20 .
6	Click OK .

4. In SmartConsole, install the Policy


Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this Security Gateway.

Step	Instructions
2	From the left navigation panel, click Gateways & Servers .
3	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. Click Install. The Access Control Policy must install successfully.
4	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Click Install. The Threat Prevention Policy must install successfully.

5. Test the functionality


Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click Logs & Monitor > Logs .
3	Examine the logs from this Security Gateway to make sure it inspects the traffic as expected.


Upgrading a VSX Gateway with CPUSE

 **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

 **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	Back up your current configuration (see "Backing Up and Restoring" on page 17).  Important - Back up both the Management Server and the VSX Gateway. Follow sk100395 .
2	See the "Upgrade Options and Prerequisites" on page 202 .
3	Upgrade the Management Server and Log Servers.
4	Upgrade the licenses on the VSX Gateway, if needed. See "Working with Licenses" on page 680 .
4	Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade. 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.


These upgrade scenarios are available:

- Upgrading the VSX Gateway with CPUSE to R81.20
- Clean Install of the R81.20 VSX Gateway

Upgrading the VSX Gateway with CPUSE to R81.20

1. On the Management Server, upgrade the configuration of the VSX Gateway object to R81.20

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	<p>On a Multi-Domain Server, go to the context of the <i>Main Domain Management Server</i> that manages this VSX Gateway object:</p> <pre data-bbox="469 674 1458 777">mdsend <IP Address or Name of Main Domain Management Server></pre>
4	<p>Upgrade the configuration of the VSX Gateway object to R81.20:</p> <pre data-bbox="469 857 1458 920">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"> ▪ IP address of the Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Gateway ▪ Management Server administrator's username ▪ Management Server administrator's password <p>Select your VSX Gateway.</p> <p>Select R81.20.</p> <p>For auditing purposes, save the <code>vsx_util</code> log file:</p> <ul style="list-style-type: none"> ▪ On a Security Management Server: <pre data-bbox="549 1469 1458 1572">/opt/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> ▪ On a Multi-Domain Server: <pre data-bbox="549 1626 1458 1765">/opt/CPmds-R81.20/customers/<Name_of_Domain>/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre>
5	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Gateway.

Step	Instructions
6	From the left navigation panel, click Gateways & Servers .
7	Open the VSX Gateway object.
8	From the left tree, click the General Properties page.
9	Make sure in the Platform section, the Version field shows R81.20 .
10	Click Cancel (do not click OK).  Note - If you click OK , the Management Server pushes the VSX configuration to the VSX Gateway. Because the VSX Gateway is not upgraded yet, this operation would fail.

2. Upgrade the VSX Gateway with CPUSE

See "[Installing Software Packages on Gaia](#)" on page 199 and follow the applicable action plan.

3. In SmartConsole, install the policy

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Gateway.
2	From the left navigation panel, click Gateways & Servers .
3	Install the default policy on the VSX Gateway object: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the default policy for this VSX Gateway object. This policy is called: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"><code><Name of VSX Gateway object>_VSX</code></div> Click Install.
4	Install the Threat Prevention Policy on the VSX Gateway object: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy for this VSX Gateway object. Click Install.


4. Test the functionality

Step	Instructions
1	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none">Connect to the command line on the VSX Gateway.Log in to the Expert mode.Run: <pre data-bbox="549 465 1460 528">vsx stat -v</pre>
2	<p>Connect with SmartConsole to the R81.20 Security Management Server or each <i>Target</i> Domain Management Server that manages the Virtual Systems on this VSX Gateway.</p>
3	<p>From the left navigation panel, click Logs & Monitor > Logs.</p>
4	<p>Examine the logs from the Virtual Systems on this VSX Gateway to make sure they inspect the traffic as expected.</p>

Clean Install of the R81.20 VSX Gateway


1. On the Management Server, upgrade the configuration of the VSX Gateway object to R81.20

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	<p>On a Multi-Domain Server, go to the context of the <i>Main Domain Management Server</i> that manages this VSX Gateway object:</p> <pre data-bbox="469 674 1458 775">mdsend <IP Address or Name of Main Domain Management Server></pre>
4	<p>Upgrade the configuration of the VSX Gateway object to R81.20:</p> <pre data-bbox="469 857 1458 920">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"> ▪ IP address of the Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Gateway ▪ Management Server administrator's username ▪ Management Server administrator's password <p>Select your VSX Gateway.</p> <p>Select R81.20.</p> <p>For auditing purposes, save the <code>vsx_util</code> log file:</p> <ul style="list-style-type: none"> ▪ On a Security Management Server: <pre data-bbox="549 1469 1458 1570">/opt/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre> ▪ On a Multi-Domain Server: <pre data-bbox="549 1626 1458 1760">/opt/CPmds-R81.20/customers/<Name_of_Domain>/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_HH_MM.log</pre>
5	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Gateway.

Step	Instructions
6	From the left navigation panel, click Gateways & Servers .
7	Open the VSX Gateway object.
8	From the left tree, click the General Properties page.
9	Make sure in the Platform section, the Version field shows R81.20 .
10	Click Cancel (do not click OK).  Note - If you click OK , the Management Server pushes the VSX configuration to the VSX Gateway. Because the VSX Gateway is not upgraded yet, this operation would fail.


2. On the VSX Gateway, perform a Clean Install of R81.20

 **Important** - You must reboot the VSX Gateway after the upgrade or clean install.

Installation Method	Instructions
Clean Install of R81.20 with CPUSE	See " Installing Software Packages on Gaia " on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install . See sk92449 for detailed steps.
Clean Install of R81.20 from scratch	Follow " Installing a VSX Gateway " on page 117 - only the step " Install the VSX Gateway ".  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Gateway (prior to the upgrade).

3. Reconfigure the VSX Gateway

Step	Instructions
1	Configure the required settings on the VSX Gateway. For more information, see the R81.20 CLI Reference Guide - Chapter <i>VSX Commands</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i> .

Step	Instructions
2	Connect to the command line on the R81.20 Security Management Server or Multi-Domain Server that manages this VSX Gateway.
3	Log in to the Expert mode.
4	On Multi-Domain Server, go to the context of the <i>Main Domain Management Server</i> that manages this VSX Gateway: <pre>mdsensv <IP Address or Name of Main Domain Management Server></pre>
5	Restore the VSX configuration: <pre>vsx_util reconfigure</pre> <p>Follow the instructions on the screen.</p> <p> Important - Enter the same Activation Key you entered during the First Time Configuration Wizard of the VSX Gateway.</p>
6	Configure the required settings on the VSX Gateway: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

4. Test the functionality

Step	Instructions
1	Examine the VSX configuration: <ol style="list-style-type: none"> a. Connect to the command line on the VSX Gateway. b. Log in to the Expert mode. c. Run: <pre>vsx stat -v</pre>
2	Connect with SmartConsole to the R81.20 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 Logs & Monitor > Logs .
4	Examine the logs from the Virtual Systems on this VSX Gateway to make sure they inspect the traffic as expected.

For more information, see the:

- [R81.20 VSX Administration Guide](#).
- [R81.20 CLI Reference Guide](#).

Upgrading ClusterXL, VSX Cluster, or VRRP Cluster


This section provides instructions to upgrade a cluster:

- ["Planning a Cluster Upgrade" on page 418](#)
- ["Multi-Version Cluster \(MVC\) Upgrade" on page 424](#)
- ["Minimum Effort Upgrade" on page 472](#)
- ["Minimum Downtime Upgrade" on page 487](#)


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)
-  **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

Planning a Cluster Upgrade

 **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

 **Important** - Before you upgrade Cluster Members:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See "Upgrade Options and Prerequisites" on page 202 .
3	Upgrade the Management Server and Log Servers.
4	Upgrade the licenses on the Cluster Members, if needed. See "Working with Licenses" on page 680 .
5	If you upgrade a VSX Cluster, then on the Management Server you must upgrade the configuration of the VSX Cluster object to R81.20.
6	<p>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</p> <p>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.</p> <p>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.</p>
7	<p>Make sure the configuration and the values of the required kernel parameters are the same on all Cluster Members.</p> <p>Log in to the Expert mode on <i>each</i> Cluster Member and run the applicable commands (see below).</p> <p> Note - For more information, see sk25977.</p>

Applicable commands and required kernel parameters

Mode	Applicable Command and Parameters
Cluster Members	<pre data-bbox="486 331 1461 394">cphaprob mmagic</pre> <p data-bbox="486 405 1110 439">Examine the value in the "MAC magic" field.</p> <p data-bbox="486 450 1265 483">Examine the value in the "MAC forward magic" field.</p>
VSX Cluster Members	<pre data-bbox="486 521 1461 577">fw ctl get int fwha_add_vsid_to_ccp_mac</pre> <pre data-bbox="486 589 1461 685">grep fwha_add_vsid_to_ccp_mac \$FWDIR/boot/modules/fwkernel.conf</pre> <p data-bbox="486 696 1433 768">Examine the value of the kernel parameter "fwha_add_vsid_to_ccp_mac".</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
<p>"Multi-Version Cluster (MVC) Upgrade" on page 424</p>	<p>Select this method, if connectivity is of utmost concern. Connection failover is guaranteed - no connections are dropped. Connections that were initiated before the upgrade are synchronized with the upgraded Security Gateways and cluster members, so that no connections are dropped. 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. Duration of this upgrade is short.</p>	<p>This upgrade method supports only specific upgrade paths. Many types of connections do not survive after failover to upgraded Cluster Member. See:</p> <ul style="list-style-type: none"> ▪ "Supported Versions in Multi-Version Cluster" on page 425 ▪ "Multi-Version Cluster Limitations" on page 427.

Upgrade Method	Instructions	Maintenance Window (downtime)	Limitations
<p><i>"Minimum Effort Upgrade" on page 472 (Simple Upgrade)</i></p>	<p>Select this method, if you have a period of time, during which network downtime is allowed. This method is the simplest, because it lets you upgrade each Cluster Member as an independent Security Gateway. All connections that were initiated before the upgrade, are dropped during the upgrade. 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. Duration of this upgrade is as long as it takes to upgrade all Cluster Members.</p>	<p>None</p>

Upgrade Method	Instructions	Maintenance Window (downtime)	Limitations
"Minimum Downtime Upgrade" on page 487	<p>Select this method, if you cannot have any network downtime and need to complete the upgrade quickly, with a minimum 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>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, because Cluster Members that run different Check Point software versions, cannot synchronize connections.</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>Duration of this upgrade is relatively short.</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 424).

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	Perform these steps: <ol style="list-style-type: none"> a. Connect over the console to the Cluster Member. b. Physically disconnect the Cluster Member from the network (disconnect all cables).
2	Perform these steps: <ol style="list-style-type: none"> a. Connect over the console to the Cluster Member. b. Log in to Gaia Clish.. c. Shut down all interfaces: <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>set interface <Name of Interface> state off</pre> </div>

For more information, see [sk42096](#).

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 (Zero Downtime Upgrade) and test the new version on some of the Cluster Members before you decide to upgrade the rest of the Cluster Members.

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>cphaprob state</pre> <ul style="list-style-type: none"> a. All Cluster Members must be operational: <ul style="list-style-type: none"> ▪ In the High Availability mode: <ul style="list-style-type: none"> One Cluster Member must be in the Active state All other Cluster Members must be in the Standby state ▪ In the Load Sharing mode: <ul style="list-style-type: none"> All Cluster Members must be in the Active state b. All Cluster Members must agree upon the states of all Cluster Members.
2	<p>Back up your current configuration (see "Backing Up and Restoring" on page 17).</p> <p> Important - If you upgrade a VSX Cluster, then back up both the Management Server and the VSX Cluster Members. Follow sk100395: How to backup and restore VSX Gateway.</p>
3	<p>See "Upgrade Options and Prerequisites" on page 202.</p>
4	<p>See "Supported Versions in Multi-Version Cluster" on the next page to know if you must install a Jumbo Hotfix Accumulator.</p>
5	<p>See "Planning a Cluster Upgrade" on page 418.</p>
6	<p>You must upgrade the Management Server and Log Servers.</p> <ul style="list-style-type: none"> ▪ See "Upgrade of Security Management Servers and Log Servers" on page 224. ▪ See "Upgrade of Multi-Domain Servers and Multi-Domain Log Servers" on page 260.
7	<p>Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.</p>

Supported Versions in Multi-Version Cluster

The Multi-Version Cluster (MVC) in an R81.20 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:

- R81.20 and R80.10 (or higher)*
- R81.20 and R77.30

*For supported upgrade paths, see the [R81.20 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
R81.20	Version X

"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 [R81.20 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 [Jumbo Hotfix Accumulator for R80.20](#)).
 - On Cluster Members R80.10, you must install R80.10 Jumbo Hotfix Accumulator Take 215 or higher (see [Jumbo Hotfix Accumulator for R80.10](#)).

The table shows the allowed combinations of Cluster Member versions:

Member 1	Member 2	Member 3	Member 4	Member 5
R81.20	Version X	Version X	Version X	Version X
R81.20	R81.20	Version X	Version X	Version X
R81.20	R81.20	R81.20	Version X	Version X

Member 1	Member 2	Member 3	Member 4	Member 5
R81.20	R81.20	R81.20	R81.20	<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 [R81.20 Release Notes](#).

Multi-Version Cluster Limitations

Specific limitations apply to Multi-Version Cluster.

General limitations in Multi-Version Cluster configuration

- The Multi-Version Cluster (MVC) upgrade does **not** support the replacement of the hardware (replacing the entire cluster member).

The MVC upgrade supports only multi-version software.

- 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.

- Multi-Version Cluster (MVC) does not support Cluster Members with Dynamically Assigned IP Addresses (DAIP).

Procedure

 **Important** - In a VSX Cluster, it is possible to install policy **only** on the *upgraded* VSX Cluster Members that run R81.20. After you change the version of the VSX Cluster object to R81.20, 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 R81.20:

On the **General Properties** page > in the **Platform** section > in the **Version** field, select **R81.20** > click **OK**.

3. Install policy on the *upgraded* Cluster Members that run R81.20:
 - 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* R81.20 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 *oldCluster* 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 *oldCluster* Members.
- Fails on the *upgradedR81.20Cluster* 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 R81.20 Cluster Member to an R77.30 Cluster Member, all VPN connections on an R81.20 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 R81.20 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 [R81.20 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 446](#).

 **Important** - Before you upgrade a Cluster:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See "Upgrade Options and Prerequisites" on page 202 .
3	Upgrade the Management Server and Log Servers.
4	See "Planning a Cluster Upgrade" on page 418 .
5	Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.

 **Note** - MVC supports Cluster Members with different Gaia kernel editions (R81.20 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 R81.20.
2. On the Cluster Member **M3**:
 - a. Upgrade to R81.20

Note - If you perform a Clean Install of R81.20, then you must establish SIC in SmartConsole with this Cluster Member and install Access Control Policy on it
 - 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 R81.20

Note - If you perform a Clean Install of R81.20, then you must establish SIC in SmartConsole with this Cluster Member and install Access Control Policy on it
 - 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 R81.20


Note - If you perform a Clean Install of R81.20, 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:



1. In SmartConsole, change the version of the cluster object

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the Cluster object.
4	From the left tree, click the General Properties page.
5	In the Platform section > Version field, select R81.20 .
6	Click OK to close the Gateway Cluster Properties window.

2. On the Cluster Member M3, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

 **Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	See "Installing Software Packages on Gaia" on page 199 . Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Upgrade . See sk92449 for detailed steps.
Clean Install of R81.20 with CPUSE	See "Installing Software Packages on Gaia" on page 199 . Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install . See sk92449 for detailed steps.  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).

Installation Method	Instructions
Clean Install of R81.20 from scratch	<p data-bbox="603 309 1011 342">Installing a Cluster Member</p> <p data-bbox="603 349 1461 425">Follow "Installing a ClusterXL Cluster" on page 124 - only the step <i>"Install the Cluster Members"</i>.</p> <p data-bbox="603 434 1453 589"> Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p data-bbox="603 629 1110 663">Installing a VRRP Cluster Member</p> <p data-bbox="603 669 1409 745">Follow "Installing a VRRP Cluster" on page 160 - only the step <i>"Install the VRRP Cluster Members"</i>.</p> <p data-bbox="603 754 1453 909"> Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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

i Important - This step is required only if you performed a Clean Install of R81.20 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

4. In SmartConsole, install the Access Control Policy on the R81.20 Cluster Member M3

i Important - This step is required only if you performed a Clean Install of R81.20 on the Cluster Member **M3**.

Step	Instructions
1	Click Install Policy .
2	In the Install Policy window: <ol style="list-style-type: none"> In the Policy field, select the applicable Access Control Policy. In the Install Mode section, select these two options: <ul style="list-style-type: none"> ▪ Select Install on each selected gateway independently. ▪ Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster. Click Install.
3	The Access Control Policy installation: <ul style="list-style-type: none"> ▪ Succeeds on the <i>upgraded</i> Cluster Member M3. ▪ Fails on the <i>old</i> Cluster Members M1 and M2 with a warning. Ignore this warning.

5. On the R81.20 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"> ▪ In Gaia Clish: <pre>set cluster member mvc on</pre> ▪ In the Expert mode: <pre>cphaconf mvc on</pre>
3	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> ▪ In Gaia Clish: <pre>show cluster members mvc</pre> ▪ In the Expert mode: <pre>cphaprob mvc</pre>


6. In SmartConsole, install the Access Control Policy on the R81.20 Cluster Member M3




Step	Instructions
1	Click Install Policy .
2	In the Install Policy window: <ol style="list-style-type: none"> In the Policy field, select the applicable Access Control Policy. In the Install Mode section, select these two options: <ul style="list-style-type: none"> Select Install on each selected gateway independently. Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster. Click Install.
3	The Access Control Policy installation: <ul style="list-style-type: none"> Succeeds on the <i>upgraded</i> Cluster Member M3. Fails on the <i>old</i> Cluster Members M1 and M2 with a warning. Ignore this warning.

7. 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"> In Gaia Clish, run: <pre>show cluster state</pre> In the Expert mode, run: <pre>cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> In the High Availability mode, one of the upgraded Cluster Members (M2 or M3) changes its cluster state to Active. The other upgraded Cluster Member (M2 or M3) changes its cluster state to Standby. In the Load Sharing modes, all Cluster Members must be in the Active state.

8. On the Cluster Member M2, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

 **Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>
Clean Install of R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.</p> <p> Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 from scratch	<p>Installing a Cluster Member</p> <p>Follow "Installing a ClusterXL Cluster" on page 124 - only the step <i>"Install the Cluster Members"</i>.</p> <p> Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p>Installing a VRRP Cluster Member</p> <p>Follow "Installing a VRRP Cluster" on page 160 - only the step <i>"Install the VRRP Cluster Members"</i>.</p> <p> Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p>

9. In SmartConsole, establish SIC with the Cluster Member M2

i Important - This step is required only if you performed a Clean Install of R81.20 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

10. In SmartConsole, install the Access Control Policy on the R81.20 Cluster Member M3 and M2

Important - This step is required only if you performed a Clean Install of R81.20 on the Cluster Member **M2**.

Step	Instructions
1	Click Install Policy .
2	In the Install Policy window: <ol style="list-style-type: none"> In the Policy field, select the applicable Access Control Policy. In the Install Mode section, select these two options: <ul style="list-style-type: none"> Select Install on each selected gateway independently. Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster. Click Install.
3	The Access Control Policy installation: <ul style="list-style-type: none"> Succeeds on the <i>upgraded</i> Cluster Members M3 and M2. Fails on the <i>old</i> Cluster Member M1 with a warning. Ignore this warning.

11. On the R81.20 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"> In Gaia Clish: <pre>set cluster member mvc on</pre> In the Expert mode: <pre>cphaconf mvc on</pre>
3	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> In Gaia Clish: <pre>show cluster members mvc</pre> In the Expert mode: <pre>cphaprob mvc</pre>


12. In SmartConsole, install the Access Control Policy on the R81.20 Cluster Members M3 and M2




Step	Instructions
1	Click Install Policy .
2	In the Install Policy window: <ol style="list-style-type: none"> In the Policy field, select the applicable Access Control Policy. In the Install Mode section, select these two options: <ul style="list-style-type: none"> Select Install on each selected gateway independently. Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster. Click Install.
3	The Access Control Policy installation: <ul style="list-style-type: none"> Succeeds on the <i>upgraded</i> Cluster Members M3 and M2. Fails on the <i>old</i> Cluster Member M1 with a warning. Ignore this warning.

13. 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"> In Gaia Clish, run: <pre>show cluster state</pre> In the Expert mode, run: <pre>cphaprob state</pre> <p>Important:</p> <ul style="list-style-type: none"> In the High Availability mode, one of the upgraded Cluster Members (M2 or M3) changes its cluster state to Active. The other upgraded Cluster Member (M2 or M3) changes its cluster state to Standby. In the Load Sharing modes, all Cluster Members must be in the Active state.

14. On the old Cluster Member M1, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

 **Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>
Clean Install of R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.</p> <p> Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 from scratch	<p>Installing a Cluster Member</p> <p>Follow "Installing a ClusterXL Cluster" on page 124 - only the step "Install the Cluster Members".</p> <p> Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p>Installing a VRRP Cluster Member</p> <p>Follow "Installing a VRRP Cluster" on page 160 - only the step "Install the VRRP Cluster Members".</p> <p> Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p>

15. In SmartConsole, establish SIC with the Cluster Member M1

i Important - This step is required only if you performed a Clean Install of R81.20 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

16. In SmartConsole, install the Access Control Policy and Threat Prevention Policy on the Cluster object

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Install the Access Control Policy: <ol style="list-style-type: none">Click Install Policy.In the Policy field, select the applicable Access Control Policy.In the Install Mode section, select these two options:<ul style="list-style-type: none">▪ Install on each selected gateway independently▪ For gateway clusters, if installation on a cluster member fails, do not install on that clusterClick Install.The Access Control Policy must install successfully on all the Cluster Members.
4	Install the Threat Prevention Policy: <ol style="list-style-type: none">Click Install Policy.In the Policy field, select the applicable Threat Prevention Policy.Click Install.The Threat Prevention Policy must install successfully on all the Cluster Members.

17. 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"> ■ In Gaia Clish, run: <pre>show cluster state</pre> ■ In the Expert mode, run: <pre>cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ■ All Cluster Members must show the same information about the states of all Cluster Members. ■ In the High Availability mode, one Cluster Member must be in the Active state, and all other Cluster Members must be in Standby state. ■ In the Load Sharing modes, all Cluster Members must be in the Active state.

18. On each Cluster Member, disable the MVC mechanism

Step	Instructions
1	Connect to the command line on each Cluster Member.
2	<p>Disable the MVC Mechanism:</p> <ul style="list-style-type: none"> ■ In Gaia Clish: <pre>set cluster member mvc off</pre> ■ In the Expert mode: <pre>cphaconf mvc off</pre>
3	<p>Examine the state of the MVC Mechanism:</p> <ul style="list-style-type: none"> ■ In Gaia Clish: <pre>show cluster members mvc</pre> ■ In the Expert mode: <pre>cphaprob mvc</pre>

19. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Logs & Monitor > Logs .
3	Examine the logs from this Cluster to make sure it inspects the traffic as expected.

For more information, see the:

- [R81.20 ClusterXL Administration Guide](#).
- [R81.20 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 430](#).

Important - Before you upgrade a VSX Cluster:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See "Upgrade Options and Prerequisites" on page 202 .
3	Upgrade the Management Server and Log Servers.
4	See "Planning a Cluster Upgrade" on page 418 .
5	Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.

Note - MVC supports VSX Cluster Members with different Gaia kernel editions (R81.20 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 R81.20.
2. On the VSX Cluster Member **M3**:
 - a. Upgrade to R81.20

Note - If you perform a Clean Install of R81.20, 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 R81.20 VSX Cluster Member **M3**
4. On the next VSX Cluster Member **M2**:
 - a. Upgrade to R81.20

Note - If you perform a Clean Install of R81.20, 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 R81.20 VSX Cluster Members **M3** and **M2**.
6. On the remaining VSX Cluster Member **M1**:
 - Upgrade to R81.20

Note - If you perform a Clean Install of R81.20, 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 R81.20



Follow the [R81.20 VSX Administration Guide](#) > Chapter *Command Line Reference* > Section *vsx_util* > Section *vsx_util upgrade*.

2. On the VSX Cluster Member M3, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

i Important - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>

Installation Method	Instructions
Clean Install of R81.20 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>"vsx_util reconfigure"</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

Installation Method	Instructions
Clean Install of R81.20 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. Follow "Installing a VSX Cluster" on page 151 - only the step <i>"Install the VSX Cluster Members"</i>. <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>"vsx_util reconfigure"</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

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>i Important:</p> <ul style="list-style-type: none"> Make sure all the configured Virtual Devices are loaded. Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> In Gaia Clish, run: <pre>set virtual-system 0 show cluster state</pre> In the Expert mode, run: <pre>vsenv 0 cphaprob state</pre>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> In Gaia Clish, run: <pre>set virtual-system 0 show cluster members interfaces all</pre> In the Expert mode, run: <pre>vsenv 0 cphaprob -a if</pre>

- i 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 R81.20 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">▪ In Gaia Clish:<pre>set virtual-system 0</pre>▪ In the Expert mode:<pre>vsenv 0</pre>
3	Enable the MVC Mechanism: <ul style="list-style-type: none">▪ In Gaia Clish:<pre>set cluster member mvc on</pre>▪ In the Expert mode:<pre>cphaconf mvc on</pre>
4	Examine the state of the MVC Mechanism: <ul style="list-style-type: none">▪ In Gaia Clish:<pre>show cluster members mvc</pre>▪ In the Expert mode:<pre>cphaprob mvc</pre>

5. In SmartConsole, install the Access Control Policy on the R81.20 VSX Cluster Member M3

Step	Instructions
1	Click Install Policy .
2	In the Install Policy window: <ol style="list-style-type: none">In the Policy field, select the applicable Access Control Policy.In the Install Mode section, select these two options:<ul style="list-style-type: none">Select Install on each selected gateway independently.Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster.Click Install.
3	The Access Control Policy installation: <ul style="list-style-type: none">Succeeds on the <i>upgraded</i> VSX Cluster Member M3.Fails on the <i>old</i> VSX Cluster Members M1 and M2 with a warning. Ignore this warning.

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 data-bbox="432 488 1275 551">vsx stat -v</pre> <p data-bbox="432 562 1289 763">  Important: <ul style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy. </p>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 882 1275 987">set virtual-system 0 show cluster state</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1032 1275 1137">vsenv 0 cphaprob state</pre>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 1263 1275 1368">set virtual-system 0 show cluster members interfaces all</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1413 1275 1518">vsenv 0 cphaprob -a if</pre>



**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 R81.20 with CPUSE, or perform a Clean Install of R81.20

-  **Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>
Clean Install of R81.20 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). Run the <code>vsx_util reconfigure</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <code>vsx_util</code> > Section <code>vsx_util reconfigure</code>.  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

Installation Method	Instructions
Clean Install of R81.20 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. Follow "Installing a VSX Cluster" on page 151 - only the step "Install the VSX Cluster Members". <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>vsx_util reconfigure</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <code>vsx_util</code> > Section <code>vsx_util reconfigure</code>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

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 data-bbox="432 488 1275 551">vsx stat -v</pre> <p data-bbox="432 562 1289 763">  Important: <ul style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy. </p>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 882 1275 987">set virtual-system 0 show cluster state</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1032 1275 1137">vsenv 0 cphaprob state</pre>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 1263 1275 1368">set virtual-system 0 show cluster members interfaces all</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1413 1275 1518">vsenv 0 cphaprob -a if</pre>

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 R81.20 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"> ▪ In Gaia Clish: <pre>set virtual-system 0</pre> ▪ In the Expert mode: <pre>vsenv 0</pre>
3	Enable the MVC Mechanism: <ul style="list-style-type: none"> ▪ In Gaia Clish: <pre>set cluster member mvc on</pre> ▪ In the Expert mode: <pre>cphaconf mvc on</pre>
4	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> ▪ In Gaia Clish: <pre>show cluster members mvc</pre> ▪ In the Expert mode: <pre>cphaprob mvc</pre>

10. In SmartConsole, install the Access Control Policy on the R81.20 VSX Cluster Members M3 and M2

Step	Instructions
1	Click Install Policy .
2	In the Install Policy window: <ol style="list-style-type: none">In the Policy field, select the applicable Access Control Policy.In the Install Mode section, select these two options:<ul style="list-style-type: none">Select Install on each selected gateway independently.Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster.Click Install.
3	The Access Control Policy installation: <ul style="list-style-type: none">Succeeds on the <i>upgraded</i> VSX Cluster Members M3 and M2.Fails on the <i>old</i> VSX Cluster Member M1 with a warning. Ignore this warning.

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 data-bbox="432 488 1275 548">vsx stat -v</pre> <p data-bbox="432 562 475 607">i</p> <p data-bbox="491 562 644 595">Important:</p> <ul data-bbox="536 602 1275 757" style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.
4	Examine the cluster state in one of these ways: <ul data-bbox="472 842 767 875" style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 882 1275 987">set virtual-system 0 show cluster state</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1037 1275 1140">vsenv 0 cphaprob state</pre>
5	Examine the cluster interfaces in one of these ways: <ul data-bbox="472 1223 767 1256" style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 1263 1275 1368">set virtual-system 0 show cluster members interfaces all</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1417 1275 1520">vsenv 0 cphaprob -a if</pre>



**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 R81.20 with CPUSE, or perform a Clean Install of R81.20

 **Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>
Clean Install of R81.20 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>.  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

Installation Method	Instructions
Clean Install of R81.20 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. Follow "Installing a VSX Cluster" on page 151 - only the step "Install the VSX Cluster Members". <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>vsx_util reconfigure</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

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> <p>i Important:</p> <ul style="list-style-type: none"> Make sure all the configured Virtual Devices are loaded. Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> In Gaia Clish, run: <pre>set virtual-system 0 show cluster state</pre> In the Expert mode, run: <pre>vsenv 0 cphaprob state</pre>
5	Examine the cluster interfaces in one of these ways: <ul style="list-style-type: none"> In Gaia Clish, run: <pre>set virtual-system 0 show cluster members interfaces all</pre> In the Expert mode, run: <pre>vsenv 0 cphaprob -a if</pre>



i 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 R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Install the Access Control Policy: <ol style="list-style-type: none"> a. Click Install Policy. b. In the Policy field, select the applicable Access Control Policy. c. In the Install Mode section, select these two options: <ul style="list-style-type: none"> ▪ Install on each selected gateway independently ▪ For gateway clusters, if installation on a cluster member fails, do not install on that cluster d. Click Install. e. The Access Control Policy must install successfully on all the Cluster Members.
4	Install the Threat Prevention Policy: <ol style="list-style-type: none"> a. Click Install Policy. b. In the Policy field, select the applicable Threat Prevention Policy. c. Click Install. d. The Threat Prevention Policy must install successfully on all the Cluster Members.

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: <pre data-bbox="432 488 1278 551" style="border: 1px solid #ccc; padding: 5px;">vsx stat -v</pre> <p data-bbox="432 562 1278 768">  Important: <ul style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy. </p>
4	Examine the cluster state in one of these ways: <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 882 1278 987" style="border: 1px solid #ccc; padding: 5px;">set virtual-system 0 show cluster state</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1032 1278 1137" style="border: 1px solid #ccc; padding: 5px;">vsenv 0 cphaprob state</pre> <p data-bbox="432 1149 1278 1644">  Important: <ul style="list-style-type: none"> ▪ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members. ▪ In the High Availability mode, one VSX Cluster Member must be in the Active state, and all other VSX Cluster Members must be in Standby state. ▪ In the Virtual System Load Sharing mode, all VSX Cluster Members must be in the Active state. ▪ All Virtual Systems must show the same information about the states of all Virtual Systems. </p>

Step	Instructions
5	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"><li data-bbox="475 280 766 313">■ In Gaia Clish, run: <pre data-bbox="512 322 1278 427">set virtual-system 0 show cluster members interfaces all</pre><li data-bbox="475 436 845 470">■ In the Expert mode, run: <pre data-bbox="512 479 1278 584">vsenv 0 cphaprob -a if</pre>

**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"> In Gaia Clish: <pre>set virtual-system 0</pre> In the Expert mode: <pre>vsenv 0</pre>
3	Disable the MVC Mechanism: <ul style="list-style-type: none"> In Gaia Clish: <pre>set cluster member mvc off</pre> In the Expert mode: <pre>cphaconf mvc off</pre>
4	Examine the state of the MVC Mechanism: <ul style="list-style-type: none"> In Gaia Clish: <pre>show cluster members mvc</pre> In the Expert mode: <pre>cphaprob mvc</pre>

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 R81.20 Security Management Server or each <i>Target</i> Domain 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 R81.20 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 Logs & Monitor > Logs .
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:

- [R81.20 ClusterXL Administration Guide](#).
- [R81.20 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"> ■ In Gaia Clish, run: <pre>show cluster statistics sync</pre> ■ In the Expert mode, run: <pre>cphaprob syncstat</pre> <p>For more information, see the R81.20 ClusterXL Administration Guide > Chapter <i>Monitoring and Troubleshooting Clusters</i> - Section <i>ClusterXL Monitoring Commands</i> > Section <i>Viewing Delta Synchronization</i>.</p>
3	<p>Examine the number of concurrent connections in the Connections kernel table (ID 8158).</p> <p>In the Expert mode, run:</p> <pre>fw tab -t connections -s</pre> <p> Important - These numbers must be as close as possible on all Cluster Members.</p> <p>For more information, see the R81.20 CLI Reference Guide.</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 [R81.20 Quantum Security Gateway Guide](#) > Chapter *Kernel Debug on Security Gateway*.


Minimum Effort Upgrade


- ★ **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

This section provides instructions for Minimum Effort Upgrade (Simple Upgrade):

- ["Minimum Effort Upgrade of a Security Gateway Cluster" on page 473](#)
 - ["Minimum Effort Upgrade of a VSX Cluster" on page 479](#)
- i **Important** - You can use this upgrade method for all supported versions as described in the [R81.20 Release Notes](#).

Minimum Effort Upgrade of a Security Gateway Cluster


 **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

 **Important** - Before you upgrade a Cluster:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See "Upgrade Options and Prerequisites" on page 202 .
3	Upgrade the Management Server and Log Servers.
4	See "Planning a Cluster Upgrade" on page 418 .
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 R81.20 with CPUSE, or perform a Clean Install of R81.20

 **Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	See "Installing Software Packages on Gaia" on page 199 . Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Upgrade . See sk92449 for detailed steps.

Installation Method	Instructions
Clean Install of R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 from scratch	<p>Installing a Cluster Member</p> <p>Follow "Installing a ClusterXL Cluster" on page 124 - only the step <i>"Install the Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p>Installing a VRRP Cluster Member</p> <p>Follow "Installing a VRRP Cluster" on page 160 - only the step <i>"Install the VRRP Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p>Installing a VSX Cluster Member</p> <p>Follow "Installing a VSX Cluster" on page 151 - only the step <i>"Install the VSX Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 Security Management Server or Domain Management Server that manages this cluster.

Step	Instructions
2	From the left navigation panel, click Gateways & Servers .
3	Open the Cluster object.
4	From the left tree, click the General Properties page.
5	In the Platform section > Version field, select R81.20 .
6	Click OK to close the Gateway Cluster Properties window.

3. In SmartConsole, establish SIC with the each Cluster Member

i Important - This step is required only if you performed a Clean Install of R81.20 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

4. In SmartConsole, install the Access Control Policy and Threat Prevention Policy on the Cluster object

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. In the Install Mode section, select these two options: <ul style="list-style-type: none"> ▪ Install on each selected gateway independently ▪ For gateway clusters, if installation on a cluster member fails, do not install on that cluster Click Install. The Access Control Policy must install successfully on all the Cluster Members.
4	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Click Install. The Threat Prevention Policy must install successfully on all the Cluster Members.

5. On each Cluster Member, examine the cluster state

Step	Instructions
1	Connect to the command line on <i>each</i> Cluster Member.

Step	Instructions
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show cluster state</pre> ■ In the Expert mode, run: <pre>cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ■ All Cluster Members must show the same information about the states of all Cluster Members. ■ In the High Availability mode, one Cluster Member must be in the Active state, and all other Cluster Members must be in Standby state. ■ In the Load Sharing modes, all Cluster Members must be in the Active state.

6. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Logs & Monitor > Logs .
3	Examine the logs from this Cluster to make sure it inspects the traffic as expected.

For more information:

See the [R81.20 ClusterXL Administration Guide](#).

Minimum Effort Upgrade of a VSX Cluster

★ **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.


i **Important** - Before you upgrade a VSX Cluster:

Step	Instructions
1	Back up your current configuration (see " Backing Up and Restoring " on page 17). i Important - Back up both the Management Server and the VSX Cluster Members. Follow sk100395 .
2	See the " Upgrade Options and Prerequisites " on page 202 .
3	Upgrade the Management Server and Log Servers.
4	See " Planning a Cluster Upgrade " on page 418 .
5	Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.

Procedure:



1. On the Management Server, upgrade the configuration of the VSX Cluster object to R81.20



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</i> Management Server that manages this VSX Cluster object: <pre>mdsensv <IP Address or Name of Main Domain Management Server></pre>
4	Upgrade the configuration of the VSX Cluster object to R81.20: <pre>vsx_util upgrade</pre> This command is interactive.

Step	Instructions
	Enter these details to log in to the management database: <ul style="list-style-type: none"> ▪ IP address of the Security Management Server or <i>Main Domain</i> Management Server that manages this VSX Cluster ▪ Management Server administrator's username ▪ Management Server administrator's password
	Select your VSX Cluster.
	Select R81.20 .
	For auditing purposes, save the <code>vsx_util</code> log file: <ul style="list-style-type: none"> ▪ On a Security Management Server: <pre data-bbox="512 707 1461 808">/opt/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_ HH_MM.log</pre> ▪ On a Multi-Domain Server: <pre data-bbox="512 864 1461 999">/opt/CPmids-R81.20/customers/<Name_of_ Domain>/CPsuite-R81.20/fw1/log/vsx_util_ YYYYMMDD_HH_MM.log</pre>
5	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain</i> Management Server that manages this VSX Cluster.
6	From the left navigation panel, click Gateways & Servers .
7	Open the VSX Cluster object.
8	From the left tree, click the General Properties page.
9	Make sure in the Platform section, the Version field shows R81.20 .
10	Click Cancel (do not click OK).  Note - If you click OK , the Management Server pushes the VSX configuration to the VSX Cluster. Because the VSX Cluster is not upgraded yet, this operation would fail.

2. On each VSX Cluster Member, Upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

 **Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>
Clean Install of R81.20 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. <p> Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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"> Run the "vsx_util reconfigure" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <p> Important - 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"> Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

Installation Method	Instructions
Clean Install of R81.20 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. Follow "Installing a VSX Cluster" on page 151 - only the step <i>"Install the VSX Cluster Members"</i>. <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>"vsx_util reconfigure"</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

3. In SmartConsole, establish SIC with each VSX Cluster Member

i Important - This step is required only if you performed a Clean Install of R81.20 on this VSX Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this VSX Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

4. In SmartConsole, install the policy

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	<p>Install the default policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the default policy for this VSX Cluster object. This policy is called: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"><i><Name of VSX Cluster object>_VSX</i></div> In the Install Mode section, select these two options: <ul style="list-style-type: none"> ▪ Install on each selected gateway independently ▪ For gateway clusters, if installation on a cluster member fails, do not install on that cluster Click Install. The default policy install successfully on all the VSX Cluster Members.
4	<p>Install the Threat Prevention Policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy for this VSX Cluster object. Click Install. The Threat Prevention Policy must install successfully on all the VSX Cluster Members.

5. 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.

Step	Instructions
3	<p>Examine the VSX configuration:</p> <pre data-bbox="432 277 1278 342">vsx stat -v</pre> <p>i Important:</p> <ul style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.
4	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 674 1278 779">set virtual-system 0 show cluster state</pre> ▪ In the Expert mode, run: <pre data-bbox="512 824 1278 929">vsenv 0 cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ▪ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members. ▪ In the High Availability mode, one VSX Cluster Member must be in the Active state, and all other VSX Cluster Members must be in Standby state. ▪ In the Virtual System Load Sharing mode, all VSX Cluster Members must be in the Active state. ▪ All Virtual Systems must show the same information about the states of all Virtual Systems.
5	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 1547 1278 1653">set virtual-system 0 show cluster members interfaces all</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1697 1278 1803">vsenv 0 cphaprob -a if</pre>

6. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R81.20 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 Logs & Monitor > Logs .
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:

- [R81.20 VSX Administration Guide](#).
- [R81.20 ClusterXL Administration Guide](#).

Minimum Downtime Upgrade


This section provides instructions for Minimum Downtime (formerly, Zero Downtime) Upgrade:


- ★ **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

This section provides instructions for Zero Downtime Upgrade:

- ["Minimum Downtime Upgrade of a Security Gateway Cluster" on page 488](#)
 - ["Minimum Downtime Upgrade of a VSX Cluster" on page 501](#)
- i **Important** - You can use this upgrade method for all supported versions as described in the [R81.20 Release Notes](#).

Minimum Downtime Upgrade of a Security Gateway Cluster

 **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.




 **Important** - Before you upgrade a Cluster:


Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	See "Upgrade Options and Prerequisites" on page 202 .
3	Upgrade the Management Server and Log Servers.
4	See "Planning a Cluster Upgrade" on page 418 .
5	Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.

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 applies only to R80.30 and lower with the Linux kernel 2.6 (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.
-  **Note** - In R80.40 and above, the Cluster Control Protocol (CCP) runs only in the Unicast mode. Therefore, after the upgrade, it is not necessary to change the CCP mode.

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>  Notes: <ul style="list-style-type: none"> ▪ This change does not require a reboot. ▪ This change applies immediately and survives reboot.
4	Make sure the CCP mode is set to Broadcast: <pre>cphaprob -a if</pre>

2. On the Cluster Member M3, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

-  **Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	See "Installing Software Packages on Gaia" on page 199 . Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Upgrade . See sk92449 for detailed steps.

Installation Method	Instructions
Clean Install of R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 from scratch	<p>Installing a Cluster Member</p> <p>Follow "Installing a ClusterXL Cluster" on page 124 - only the step <i>"Install the Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p>Installing a VRRP Cluster Member</p> <p>Follow "Installing a VRRP Cluster" on page 160 - only the step <i>"Install the VRRP Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p>Installing a VSX Cluster Member</p> <p>Follow "Installing a VSX Cluster" on page 151 - only the step <i>"Install the VSX Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 M2, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

i Important - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>
Clean Install of R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 from scratch	<p>Installing a Cluster Member</p> <p>Follow "Installing a ClusterXL Cluster" on page 124 - only the step <i>"Install the Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p>Installing a VRRP Cluster Member</p> <p>Follow "Installing a VRRP Cluster" on page 160 - only the step <i>"Install the VRRP Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p>Installing a VSX Cluster Member</p> <p>Follow "Installing a VSX Cluster" on page 151 - only the step <i>"Install the VSX Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the Cluster object.
4	From the left tree, click the General Properties page.
5	In the Platform section > Version field, select R81.20 .
6	Click OK to close the Gateway Cluster Properties window.

5. In SmartConsole, establish SIC with the Cluster Member M3

i Important - This step is required only if you performed a Clean Install of R81.20 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

6. In SmartConsole, establish SIC with the Cluster Member M2

i Important - This step is required only if you performed a Clean Install of R81.20 on this Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

7. In SmartConsole, install the Access Control Policy

Step	Instructions
1	Click Install Policy .

Step	Instructions
2	In the Install Policy window: <ol style="list-style-type: none"> In the Policy field, select the applicable Access Control Policy. In the Install Mode section, configure these two options: <ul style="list-style-type: none"> ▪ Select Install on each selected gateway independently. ▪ Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster. Click Install.
3	The Access Control Policy installation: <ul style="list-style-type: none"> ▪ Succeeds on the <i>upgraded</i> Cluster Members M2 and M3. ▪ Fails on the <i>old</i> Cluster Member M1 with a warning. Ignore this warning.

8. 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"> ▪ In Gaia Clish (R80.20 and higher), run: <pre>show cluster state</pre> ▪ In the Expert mode, run: <pre>cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ▪ The cluster states of the upgraded Cluster Members M2 and M3 are Ready. ▪ The cluster state of the old Cluster Member M1 is: <ul style="list-style-type: none"> • In R80.20 and higher - Active(!). • In R80.10 and lower - Active Attention.

9. On the old Cluster Member M1, stop all Check Point services

Step	Instructions
1	Connect to the command line on the Cluster Member M1 .

Step	Instructions
2	<p>Stop all Check Point services:</p> <pre>cpstop</pre> <p>i Notes:</p> <ul style="list-style-type: none"> ▪ This forces a controlled cluster failover from the old Cluster Member M1 to one of the upgraded Cluster Members. ▪ At this moment, all connections that were initiated through the old Cluster Member M1 are dropped (because Cluster Members with different software versions cannot synchronize).

10. 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"> ▪ In Gaia Clish, run: <pre>show cluster state</pre> ▪ In the Expert mode, run: <pre>cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ▪ In the High Availability mode, one of the upgraded Cluster Members (M2 or M3) changes its cluster state to Active. The other upgraded Cluster Member (M2 or M3) changes its cluster state to Standby. ▪ In the Load Sharing modes, all Cluster Members must be in the Active state.

11. On the old Cluster Member M1, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

- i** **Important** - You must reboot the Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>
Clean Install of R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection 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 R81.20 from scratch	<p>Installing a Cluster Member</p> <p>Follow "Installing a ClusterXL Cluster" on page 124 - only the step <i>"Install the Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous Cluster Member (prior to the upgrade).</p> <p>Installing a VRRP Cluster Member</p> <p>Follow "Installing a VRRP Cluster" on page 160 - only the step <i>"Install the VRRP Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VRRP Cluster Member (prior to the upgrade).</p> <p>Installing a VSX Cluster Member</p> <p>Follow "Installing a VSX Cluster" on page 151 - only the step <i>"Install the VSX Cluster Members"</i>.</p> <p>i Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade).</p>

12. In SmartConsole, establish SIC with the Cluster Member M1

i Important - This step is required only if you performed a Clean Install of R81.20 on this Cluster Member **M1**.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of the Cluster Member M1 .
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.

13. In SmartConsole, install the Access Control Policy and Threat Prevention Policy on the Cluster object

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Gateways & Servers .

Step	Instructions
3	Install the Access Control Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Access Control Policy. In the Install Mode section, select these two options: <ul style="list-style-type: none"> ▪ Install on each selected gateway independently ▪ For gateway clusters, if installation on a cluster member fails, do not install on that cluster Click Install. The Access Control Policy must install successfully on all the Cluster Members.
4	Install the Threat Prevention Policy: <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy. Click Install. The Threat Prevention Policy must install successfully on all the Cluster Members.

14. 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"> ▪ In Gaia Clish, run: <pre>show cluster state</pre> ▪ In the Expert mode, run: <pre>cphaprob state</pre> <p>Important:</p> <ul style="list-style-type: none"> ▪ All Cluster Members must show the same information about the states of all Cluster Members. ▪ In the High Availability mode, one Cluster Member must be in the Active state, and all other Cluster Members must be in Standby state. ▪ In the Load Sharing modes, all Cluster Members must be in the Active state.

15. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or Domain Management Server that manages this cluster.
2	From the left navigation panel, click Logs & Monitor > Logs .
3	Examine the logs from this Cluster to make sure it inspects the traffic as expected.

For more information:

See the [R81.20 ClusterXL Administration Guide](#).

Minimum Downtime Upgrade of a VSX Cluster

★ **Best Practice** - Use the Central Deployment in SmartConsole. For more information, see the [R81.20 Security Management Administration Guide](#) > Chapter *Managing Gateways* > Section *Central Deployment of Hotfixes and Version Upgrades*.

i **Important** - Before you upgrade a VSX Cluster:

Step	Instructions
1	Back up your current configuration (see " Backing Up and Restoring " on page 17). i Important - Back up both the Management Server and the VSX Cluster Members. Follow sk100395 .
2	See the " Upgrade Options and Prerequisites " on page 202 .
3	Upgrade the Management Server and Log Servers.
4	See " Planning a Cluster Upgrade " on page 418 .
5	Schedule a full maintenance window to make sure you can make all the custom configurations again after the upgrade.


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 R81.20

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>mdsensv <IP Address or Name of Main Domain Management Server></pre>

Step	Instructions
4	<p>Upgrade the configuration of the VSX Cluster object to R81.20:</p> <pre data-bbox="432 280 1458 340">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"> ▪ IP address of the Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Cluster ▪ Management Server administrator's username ▪ Management Server administrator's password <p>Select your VSX Cluster.</p> <p>Select R81.20.</p> <p>For auditing purposes, save the <code>vsx_util</code> log file:</p> <ul style="list-style-type: none"> ▪ On a Security Management Server: <pre data-bbox="512 896 1458 992">/opt/CPsuite-R81.20/fw1/log/vsx_util_YYYYMMDD_ HH_MM.log</pre> ▪ On a Multi-Domain Server: <pre data-bbox="512 1043 1458 1184">/opt/CPmds-R81.20/customers/<Name_of_ Domain>/CPsuite-R81.20/fw1/log/vsx_util_ YYYYMMDD_HH_MM.log</pre>
5	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Cluster.
6	From the left navigation panel, click Gateways & Servers .
7	Open the VSX Cluster object.
8	From the left tree, click the General Properties page.
9	Make sure in the Platform section, the Version field shows R81.20 .
10	<p>Click Cancel (do not click OK).</p> <p> Note - If you click OK, 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.
3	Change the CCP mode to Broadcast: <pre>cphaconf set_ccp broadcast</pre> <p>i Notes:</p> <ul style="list-style-type: none"> ■ This change does not require a reboot. ■ This change applies immediately and survives reboot.
4	Make sure the CCP mode is set to Broadcast: <pre>cphaprob -a if</pre>

3. On the VSX Cluster Member M3, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

- i** **Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	See "Installing Software Packages on Gaia" on page 199 . Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Upgrade . See sk92449 for detailed steps.



Installation Method	Instructions
Clean Install of R81.20 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>vsx_util reconfigure</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.



Installation Method	Instructions
Clean Install of R81.20 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> Follow "Installing a VSX Cluster" on page 151 - only the step "Install the VSX Cluster Members". <ul style="list-style-type: none"> Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). Run the <code>vsx_util reconfigure</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter Command Line Reference > Section <code>vsx_util</code> > Section <code>vsx_util reconfigure</code>. <ul style="list-style-type: none"> Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). Settings manually defined in various configuration files. Applicable Check Point configuration files.

4. On the VSX Cluster Member M2, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

- Important** - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>

Installation Method	Instructions
Clean Install of R81.20 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>"vsx_util reconfigure"</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

Installation Method	Instructions
Clean Install of R81.20 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. Follow "Installing a VSX Cluster" on page 151 - only the step "Install the VSX Cluster Members". <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the "<code>vsx_util reconfigure</code>" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

5. In SmartConsole, establish SIC with the VSX Cluster Member M3

i Important - This step is required only if you performed a Clean Install of R81.20 on this VSX Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this VSX Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

6. In SmartConsole, establish SIC with the VSX Cluster Member M2


i Important - This step is required only if you performed a Clean Install of R81.20 on this VSX Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this VSX Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

7. In SmartConsole, install the Access Control Policy

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Click Install Policy .
4	<p>In the Install Policy window:</p> <ol style="list-style-type: none"> In the Policy field, select the default policy for this VSX Cluster object. This policy is called: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"><code><Name of VSX Cluster object>_VSX</code></div> In the Install Mode section, configure these two options: <ul style="list-style-type: none"> ▪ Select Install on each selected gateway independently. ▪ Clear For gateway clusters, if installation on a cluster member fails, do not install on that cluster. Click Install.
5	<p>The policy installation:</p> <ul style="list-style-type: none"> ▪ Succeeds on the <i>upgraded</i> VSX Cluster Members M2 and M3. ▪ Fails on the <i>old</i> VSX Cluster Member M1 with a warning. Ignore this warning.

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	<p>Examine the VSX configuration:</p> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"><code>vsx stat -v</code></div> <p> Important:</p> <ul style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.

Step	Instructions
4	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> ■ In Gaia Clish (R80.20 and higher), run: <pre>set virtual-system 0 show cluster state</pre> ■ In the Expert mode, run: <pre>vsenv 0 cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ■ The cluster states of the upgraded VSX Cluster Members M2 and M3 are Ready. ■ The cluster state of the old VSX Cluster Member M1 is: <ul style="list-style-type: none"> • In R80.20 and higher - Active(!). • In R80.10 and lower - Active Attention.

9. 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 M1 .
2	<p>Stop all Check Point services:</p> <pre>cpstop</pre> <p>i Notes:</p> <ul style="list-style-type: none"> ■ This forces a controlled cluster failover from the old VSX Cluster Member M1 to one of the upgraded VSX Cluster Members. ■ At this moment, all connections that were initiated through the old VSX Cluster Member M1 are dropped (because VSX Cluster Members with different software versions cannot synchronize).

10. 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 M2 and M3 .



Step	Instructions
2	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show cluster state</pre> ■ In the Expert mode, run: <pre>cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ■ One of the VSX Cluster Members (M2 or M3) changes its cluster state to Active. ■ The other VSX Cluster Member (M2 or M3) changes its cluster state to Standby.

11. On the old VSX Cluster Member M1, upgrade to R81.20 with CPUSE, or perform a Clean Install of R81.20

i Important - You must reboot the VSX Cluster Member after the upgrade or clean install.

Installation Method	Instructions
Upgrade to R81.20 with CPUSE	<p>See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation.</p> <p>In local installation, select the R81.20 package and perform Upgrade. See sk92449 for detailed steps.</p>

Installation Method	Instructions
Clean Install of R81.20 with CPUSE	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. See "Installing Software Packages on Gaia" on page 199. Follow the applicable action plan for the local or central installation. In local installation, select the R81.20 package and perform Clean Install. See sk92449 for detailed steps. <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the <code>"vsx_util reconfigure"</code> command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

Installation Method	Instructions
Clean Install of R81.20 from scratch	<p>Follow these steps:</p> <ol style="list-style-type: none"> a. Follow "Installing a VSX Cluster" on page 151 - only the step "Install the VSX Cluster Members". <ul style="list-style-type: none">  Important - In the Gaia First Time Configuration Wizard, for the Management Connection IP address, you must use the same IP address as was used by the previous VSX Cluster Member (prior to the upgrade). b. Run the "<code>vsx_util reconfigure</code>" command on the Management Server to push the VSX configuration to this VSX Cluster Member. See the R81.20 VSX Administration Guide > Chapter <i>Command Line Reference</i> > Section <i>vsx_util</i> > Section <i>vsx_util reconfigure</i>. <ul style="list-style-type: none">  Important - You must enter the same Activation Key you entered during the Gaia First Time Configuration Wizard of this VSX Cluster Member. c. Configure the required settings on this VSX Cluster Member: <ul style="list-style-type: none"> ▪ OS configuration (for example, DNS, NTP, DHCP, Dynamic Routing, DHCP Relay, and so on). ▪ Settings manually defined in various configuration files. ▪ Applicable Check Point configuration files.

12. In SmartConsole, establish SIC with the VSX Cluster Member M1

i Important - This step is required only if you performed a Clean Install of R81.20 on this VSX Cluster Member.

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main</i> Domain Management Server that manages this VSX Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	Open the cluster object.
4	From the left tree, click Cluster Members .
5	Select the object of this VSX Cluster Member.
6	Click Edit .
7	On the General tab, click the Communication button.
8	Click Reset .
9	In the One-time password field, enter the same Activation Key you entered during the First Time Configuration Wizard of the Cluster Member.
10	In the Confirm one-time password field, enter the same Activation Key again.
11	Click Initialize .
12	The Trust state field must show Trust established .
13	Click Close to close the Communication window.
14	Click OK to close the Cluster Member Properties window.
15	Click OK to close the Gateway Cluster Properties window.
16	Publish the SmartConsole session.

13. In SmartConsole, install the policy

Step	Instructions
1	Connect with SmartConsole to the R81.20 Security Management Server or <i>Main Domain Management Server</i> that manages this VSX Cluster.
2	From the left navigation panel, click Gateways & Servers .
3	<p>Install the default policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the default policy for this VSX Cluster object. This policy is called: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"><i><Name of VSX Cluster object>_VSX</i></div> In the Install Mode section, select these two options: <ul style="list-style-type: none"> ▪ Install on each selected gateway independently ▪ For gateway clusters, if installation on a cluster member fails, do not install on that cluster Click Install. The default policy install successfully on all the VSX Cluster Members.
4	<p>Install the Threat Prevention Policy on the VSX Cluster object:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable Threat Prevention Policy for this VSX Cluster object. Click Install. The Threat Prevention Policy must install successfully on all the VSX Cluster Members.

14. 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.

Step	Instructions
3	<p>Examine the VSX configuration:</p> <pre data-bbox="432 277 1278 342">vsx stat -v</pre> <p>i Important:</p> <ul style="list-style-type: none"> ▪ Make sure all the configured Virtual Devices are loaded. ▪ Make sure all Virtual Systems and Virtual Routers have SIC Trust and policy.
4	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 674 1278 779">set virtual-system 0 show cluster state</pre> ▪ In the Expert mode, run: <pre data-bbox="512 824 1278 929">vsenv 0 cphaprob state</pre> <p>i Important:</p> <ul style="list-style-type: none"> ▪ All VSX Cluster Members must show the same information about the states of all VSX Cluster Members. ▪ In the High Availability mode, one VSX Cluster Member must be in the Active state, and all other VSX Cluster Members must be in Standby state. ▪ In the Virtual System Load Sharing mode, all VSX Cluster Members must be in the Active state. ▪ All Virtual Systems must show the same information about the states of all Virtual Systems.
5	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre data-bbox="512 1547 1278 1653">set virtual-system 0 show cluster members interfaces all</pre> ▪ In the Expert mode, run: <pre data-bbox="512 1697 1278 1803">vsenv 0 cphaprob -a if</pre>

15. Test the functionality

Step	Instructions
1	Connect with SmartConsole to the R81.20 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 Logs & Monitor > Logs .
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:

- [R81.20 VSX Administration Guide](#).
- [R81.20 CLI Reference Guide](#).

Upgrading a Full High Availability Cluster

For more information, see ["Full High Availability Cluster on Check Point Appliances" on page 180](#).

To upgrade, follow the procedure ["Upgrading Security Management Servers in Management High Availability from R80.20 and higher" on page 254](#).

-  **Important** - After you upgrade a Full High Availability Cluster to R81.20, 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.

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 [R81.20 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 R81.20 Multi-Domain Servers

This procedure lets you export the entire management database from a Domain Management Server on one R81.20 Multi-Domain Server and import it on another R81.20 Multi-Domain Server.

For the list of known limitations, see [sk156072](#).

Procedure:

1. On the source Multi-Domain Server, export the Domain Management Server

- a. Run this API:

```
migrate-export-domain
```

For API documentation, see the [Check Point Management API Reference](#) - search for *migrate-export-domain*.

- b. Calculate the MD5 of the export file:

```
md5sum <Full Path to Export File>
```

2. Transfer the export file to the target Multi-Domain Server

- a. 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.

- 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 Multi-Domain Server:

```
md5sum <Full Path to Export File>
```

3. On the target Multi-Domain Server, import the Domain Management Server

- a. 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 CPCA) 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 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 [R81.20 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 R81.20 Security Management Servers

This procedure lets you export the entire management database from one R81.20 Security Management Server and import it on another R81.20 Security Management Server.


Important - Before you migrate the database:

Step	Instructions
1	Back up your current configuration (see "Backing Up and Restoring" on page 17).
2	Examine the SmartConsole sessions: <ol style="list-style-type: none"> 1. Connect with the SmartConsole to the Security Management Server. 2. From the left navigation panel, click Manage & Settings > Sessions > View Sessions. 3. You must publish or discard all sessions, for which the Changes column shows a number greater than zero. Right-click on such session and select Publish or Discard.
3	You must close all GUI clients (SmartConsole applications) connected to the source Security Management Server.

Procedure:

1. On the source R81.20 Security Management Server, export the entire management database


Step	Instructions
1	Connect to the command line on the current R81.20 Security Management Server.
2	Log in to the Expert mode.
3	Go to the <code>\$FWDIR/scripts/</code> directory: <pre>cd \$FWDIR/scripts/</pre>


Step	Instructions
4	<p>Export the management database:</p> <p>If the "Endpoint Policy Management" blade is <i>disabled</i> on this Security Management Server</p> <ul style="list-style-type: none"> ▪ And this Security Management Server <i>is</i> connected to the Internet, run: <pre data-bbox="541 465 1460 568">./migrate_server export -v R81.20 [-l -x] /<Full Path>/<Name of Exported File></pre> ▪ And this Security Management Server is not connected to the Internet, run: <pre data-bbox="541 658 1460 801">./migrate_server export -v R81.20 -skip_ upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File></pre> <p>If the "Endpoint Policy Management" blade is <i>enabled</i> on this Security Management Server</p> <ul style="list-style-type: none"> ▪ This Security Management Server <i>is</i> connected to the Internet, run: <pre data-bbox="541 1003 1460 1146">./migrate_server export -v R81.20 [-l -x] [--include-uepm-msi-files] /<Full Path>/<Name of Exported File></pre> ▪ This Security Management Server is not connected to the Internet, run: <pre data-bbox="541 1236 1460 1415">./migrate_server export -v R81.20 -skip_ upgrade_tools_check [-l -x] [--include- uepm-msi-files] /<Full Path>/<Name of Exported File></pre> <p>For details, see the R81.20 CLI Reference Guide - 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 data-bbox="432 1592 1460 1653">md5sum /<Full Path>/<Name of Database File>.tgz</pre>
6	<p>Transfer the exported databases from the source Security Management Server to an external storage:</p> <pre data-bbox="432 1776 1460 1836">/<Full Path>/<Name of Database File>.tgz</pre> <p> Note - Make sure to transfer the file in the binary mode.</p>

2. Install a new R81.20 Security Management Server

Step	Instructions
1	See the R81.20 Release Notes for requirements.
2	Perform a clean install of the R81.20 Security Management Server on another computer. See " Installing a Security Management Server " on page 65.

3. On the R81.20 Security Management Server, import the databases

Step	Instructions
1	Connect to the command line on the R81.20 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 R81.20 Security Management Server, to some directory.  Note - 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 /<Full Path>/<Name of Database File>.tgz</pre>
6	Go to the <code>\$FWDIR/scripts/</code> directory: <pre>cd \$FWDIR/scripts/</pre>

Step	Instructions
7	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Security Management Server <i>is</i> connected to the Internet, run: <pre data-bbox="512 360 1460 465">./migrate_server import -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ■ If this Security Management Server is not connected to the Internet, run: <pre data-bbox="512 555 1460 696">./migrate_server import -v R81.20 -skip_ upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p> Important - The "migrate_server import" command automatically restarts Check Point services (runs the "cpstop" and "cpstart" commands).</p> <p>For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>

4. Test the functionality on the R81.20 Security Management Server

Step	Instructions
1	Connect with SmartConsole to the R81.20 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 R81.20 Security Management Server to an R81.20 Domain Management Server

This procedure lets you export the entire management database from an R81.20 Security Management Server and import it on an R81.20 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.

- 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

- 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 17](#).
- 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 R81.20 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 R81.20 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 CPCA) 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 [R81.20 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 R81.20 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 R81.20 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 R81.20 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 R81.20 Domain Management Server to an R81.20 Security Management Server

This procedure lets you export the entire management database from a Domain Management Server on an R81.20 Multi-Domain Server and import it on an R81.20 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 17.
- 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.

- 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

- Install all updated Access Control Policies.

Prerequisites on the target Security Management Server:

- Perform a clean install of an R81.20 Security Management Server.

See ["Installing One Security Management Server only, or Primary Security Management Server in Management High Availability" on page 66](#).

- Make sure you install the required license.

Procedure:**1. On the source R81.20 Multi-Domain Server, export the Domain Management Server****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 domain
"MyDomain3" file-path "/var/log/MyDomain3_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 R81.20 Security Management Server**a. 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.

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 Multi-Domain Server:

```
md5sum /<Full Path>/<Name of Exported File>.tgz
```

3. On the target R81.20 Security Management Server, import the Domain Management Server database

Step	Instructions
1	Connect to the command line the target Security Management Server.
2	Log in to the Expert mode.

Step	Instructions
3	<p>Go to the <code>\$MDS_FWDIR/scripts/</code> directory:</p> <pre>cd \$MDS_FWDIR/scripts/</pre>
4	<p>Import the management database:</p> <ul style="list-style-type: none"> ■ If this Security Management Server <i>is</i> connected to the Internet: <pre>./migrate_server migrate_import_domain -v R81.20 [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> ■ If this Security Management Server is not connected to the Internet: <pre>./migrate_server migrate_import_domain -v R81.20 -skip_upgrade_tools_check [-l -x] /<Full Path>/<Name of Exported File>.tgz</pre> <p>For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>migrate_server</i>.</p>
5	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPM) are in the state "E" and show their PID:</p> <pre>cpwd_admin list</pre> <p>If some of the required daemons on the Security Management Server are in the state "T", then wait for 5-10 minutes, restart the Security Management Server and check again. Run these two commands:</p> <pre>cpstop cpstart</pre>

4. Configure and assign the Administrators and GUI clients

You must again configure the Security Management Server Administrators and GUI clients.

- a. Run the `cpconfig` command.
- b. Configure the **Administrators**.
- c. Configure the **GUI clients**.
- d. Exit the `cpconfig` menu.

5. Stop the source R81.20 Domain Management Server

- a. Connect to the command line on the source Multi-Domain Server.
- b. Stop the source Domain Management Server you migrated:

```
mdsstop_customer <IP address or Name of Domain  
Management Server>
```

6. Test the functionality on the target R81.20 Security Management Server

- a. Connect with SmartConsole to the target Security 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. Delete the source R81.20 Domain Management Server

Make sure you backed up the Multi-Domain Server. See ["Backing Up and Restoring" on page 17](#).

- a. Connect with SmartConsole to the source Multi-Domain Server to the **MDS** context.
- b. From the left navigation panel, click **Multi Domain > Domains**.
- c. 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.

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 R81.20 Multi-Domain Server or Multi-Domain Log Server

See ["Backing Up and Restoring" on page 17](#).

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 [R81.20 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 Check Point User Center 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 "Working with Licenses" on page 680 .

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.

Step	Instructions
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Go to the MDS context: <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">mdsend</div>

5. Stop all processes in the MDS context

Step	Instructions
1	Stop all processes in the MDS context: <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">mdsstop -m</div> <p> Important - While these process are stopped, SmartConsole cannot connect.</p>
2	Make sure all processes stopped in the MDS context: <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">mdsstat -m</div> <p>All the daemons (FWM, FWD, CPD, and CPCA) must be in the state "down".</p>

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: <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">\$MDSDIR/bin/mdscmd change-mds-ip <Current IP Address> <New IP Address> ipv4 -x</div> <p>Example:</p> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;">\$MDSDIR/bin/mdscmd change-mds-ip 192.168.20.30 172.30.40.50 ipv4 -x</div>

Step	Instructions
2	<p>Make sure the IP address is updated in the dleobjectderef_data database:</p> <ol style="list-style-type: none"> Save the applicable data from this database to a file: <pre data-bbox="512 360 1458 544">psql_client -c "select fwset from dleobjectderef_data where cpmitable='mdss' and not deleted and dlesession=0" -o /tmp/dleobject.txt cpm postgres</pre> Examine the IP address: <pre data-bbox="512 593 1458 692">cat /tmp/dleobject.txt egrep -w 'name ipaddr'</pre> <p>Example output:</p> <pre data-bbox="512 741 1458 846">:name (My_MDS_Server) :ipaddr (172.30.40.50)</pre>
3	<p>Make sure the IP address is updated in the cpnetworkobject_data database:</p> <ol style="list-style-type: none"> Save the applicable data from this database to a file: <pre data-bbox="512 1010 1458 1193">psql_client -c "select name, ipaddress4 from cpnetworkobject_data where not deleted and dlesession=0" -o /tmp/cpnetworkobject.txt cpm postgres</pre> Examine the IP address: <pre data-bbox="512 1243 1458 1305">cat /tmp/cpnetworkobject.txt</pre> <p>Example output:</p> <pre data-bbox="512 1355 1458 1496"> 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 <code>\$MDSDIR/conf/external.if</code> file:</p> <pre>cp -v \$MDSDIR/conf/external.if{, _BKP}</pre>
2	<p>Edit the current <code>\$MDSDIR/conf/external.if</code> file:</p> <pre>vi \$MDSDIR/conf/external.if</pre>
3	<p>Change the current interface name to the name of the applicable main interface.</p> <p>This is the interface, on which you configured the main IPv4 address of your Multi-Domain Server or Multi-Domain Log Server.</p>
4	<p>Save the changes and exit the Vi editor.</p>
5	<p>Go to the context of each existing Domain Management Server:</p> <pre>mdsendv <IP Address or Name of Domain Management Server></pre>
6	<p>Back up the current <code>\$FWDIR/conf/vip_index.conf</code> file:</p> <pre>cp -v \$FWDIR/conf/vip_index.conf{, _BKP}</pre>
7	<p>Edit the current <code>\$FWDIR/conf/vip_index.conf</code> file:</p> <pre>vi \$FWDIR/conf/vip_index.conf</pre>
8	<p>Change the current interface name to the name of the applicable main interface.</p> <p>This is the interface, on which you configured the main IPv4 address of your Multi-Domain Server or Multi-Domain Log Server.</p>
9	<p>Save the changes and exit the Vi editor.</p>

8. Modify the `$MDSDIR/conf/LeadingIP` file

Step	Instructions
1	<p>Back up the current <code>\$MDSDIR/conf/LeadingIP</code> file:</p> <pre>cp -v \$MDSDIR/conf/LeadingIP{, _BKP}</pre>
2	<p>Edit the current file:</p> <pre>vi \$MDSDIR/conf/LeadingIP</pre>

Step	Instructions
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	<p>Back up the current <code>\$MDSDIR/conf/mdsdb/mdss.C</code> file:</p> <pre>cp -v \$MDSDIR/conf/mdsdb/mdss.C{, _BKP}</pre>
2	<p>Edit the current <code>\$MDSDIR/conf/mdsdb/mdss.C</code> file:</p> <pre>vi \$MDSDIR/conf/mdsdb/mdss.C</pre>
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 not 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	<p>Back up the current <code>\$SMARTLOGDIR/smartlog_settings.txt</code> file:</p> <pre>cp -v \$SMARTLOGDIR/smartlog_settings.txt{, _BKP}</pre>
2	<p>Edit the current file:</p> <pre>vi \$SMARTLOGDIR/smartlog_settings.txt</pre>
3	<p>Change the current IP address to the new IP address in these parameters:</p> <ul style="list-style-type: none"> ■ Parameter : <code>server_port ()</code> ■ Section : <code>connections > Section : domain > Section : management > Parameter : name ()</code> ■ Section : <code>connections > Section : domain > Section : log_servers > Parameter : name ()</code>

Step	Instructions
4	Save the changes in the file and exit the editor.

11. Modify the `$INDEXERDIR/log_indexer_custom_settings.conf` file

Step	Instructions
1	<p>Back up the current <code>\$INDEXERDIR/log_indexer_custom_settings.conf</code> file:</p> <pre>cp -v \$INDEXERDIR/log_indexer_custom_settings.conf {, _BKP}</pre>
2	<p>Edit the current file:</p> <pre>vi \$INDEXERDIR/log_indexer_custom_settings.conf</pre>
3	<p>Change the current IP address to the new IP address in these parameters:</p> <ul style="list-style-type: none"> ▪ Parameter :server_port () ▪ Section :connections > Section :domain > Section :management > Parameter :name () ▪ Section :connections > Section :domain > Section :log_servers > Parameter :name ()
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>mgsstart -m</pre>
2	<p>Make sure all processes started in the MDS context:</p> <pre>mgsstat -m</pre> <p>All the daemons (FWM, FWD, CPD, and CPCA) 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 548.

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 541](#).
- 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 R81.20 Multi-Domain Server or Multi-Domain Log Server**

See ["Backing Up and Restoring" on page 17](#).

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.
2	Log in with the superuser credentials.
3	Log in to the Expert mode.
4	Go to the MDS context: <pre>mdsenv</pre>

4. Stop the applicable Domain Management Server or Domain Log Server

Step	Instructions
1	Stop the services: <pre>mdsstop_customer <Name or IP of Domain Management Server or Domain Log Server></pre>
2	Make sure the services stopped in the applicable context: <pre>mdsstat</pre> <p>All the daemons (FWM, FWD, CPD, and CPCA) must be in the state "down".</p>

5. Change the IP address in the MDS database

Step	Instructions
1	Change the IP address: <pre>\$MDS_TEMPLATE/scripts/change_cma_ip.sh -n <Name of Domain Management Server or Domain Log Server object> -i <New IP Address></pre> <p>Example:</p> <pre>\$MDS_TEMPLATE/scripts/change_cma_ip.sh -n My_Domain_Server -i 172.30.40.55</pre>

Step	Instructions
	<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"> Make sure the services stopped in all applicable contexts. Create a plain text file that contains pairs of server names and their new IPv4 addresses (separated with comma). Example of a file: <div data-bbox="512 483 1460 629" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>MyDomainManagementServer_1, 172.30.40.51 MyDomainManagementServer_2, 172.30.40.52 MyDomainManagementServer_3, 172.30.40.53</pre> </div> Run this command: <div data-bbox="512 678 1460 779" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>\$MDS_TEMPLATE/scripts/change_cma_ip.sh -f /<Path To>/<File></pre> </div>

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> <div data-bbox="432 1081 1460 1182" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>mdsend <Name or IP of Domain Management Server or Domain Log Server></pre> </div>
2	<p>Back up the current <code>\$SMARTLOGDIR/smartlog_settings.txt</code> file:</p> <div data-bbox="432 1261 1460 1328" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>cp -v \$SMARTLOGDIR/smartlog_settings.txt{, _BKP}</pre> </div>
3	<p>Edit the current file:</p> <div data-bbox="432 1406 1460 1473" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>vi \$SMARTLOGDIR/smartlog_settings.txt</pre> </div>
4	<p>Change the current IP address to the new IP address in these parameters:</p> <ul style="list-style-type: none"> ▪ Parameter :server_port () ▪ Section :connections > Section :domain > Section :management > Parameter :name () ▪ Section :connections > Section :domain > Section :log_servers > Parameter :name ()
5	<p>Save the changes in the file and exit the editor.</p>

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 <Name or IP of Domain Management Server or Domain Log Server></pre>
2	<p>Back up the current <code>\$INDEXERDIR/log_indexer_custom_settings.conf</code> 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"> ▪ Parameter :server_port () ▪ Section :connections > Section :domain > Section :management > Parameter :name () ▪ Section :connections > Section :domain > Section :log_servers > Parameter :name ()
5	<p>Save the changes in the file and exit the editor.</p>

8. Start the applicable Domain Management Server or Domain Log Server

Step	Instructions
1	<p>Start the services:</p> <pre>mdsstart_customer <Name or IP of Domain Management Server or Domain Log Server></pre>

Step	Instructions
2	<p>Make sure that all the required daemons (FWM, FWD, CPD, and CPCA) are in the state "up" and show their PID (the "pnd" state is also acceptable):</p> <pre data-bbox="432 356 1461 421">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="432 591 1461 815">mdsstop_customer <IP Address or Name or IP of Domain Management Server or Domain Log Server> mdsstart_customer <IP Address or Name or IP of Domain Management Server or Domain Log Server> 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 R81.20, 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 [R81.20 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 555](#)
- ["Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591](#)
- ["Security Before Firewall Activation" on page 670](#)

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.

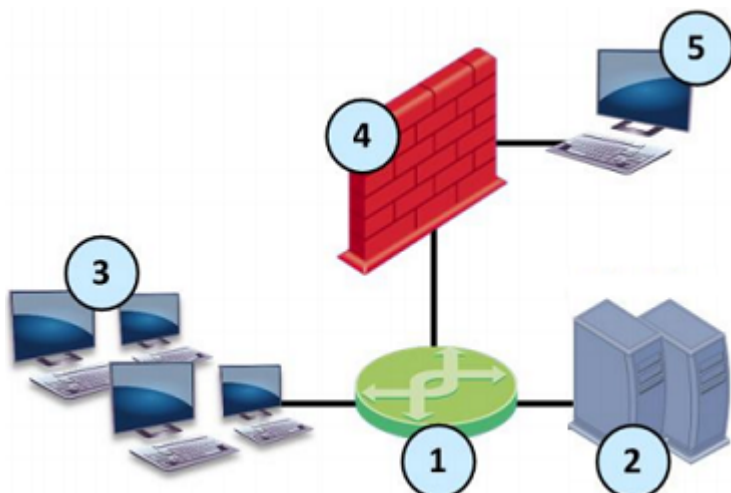
You can use the Monitor Mode:

- 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.

i **Important** - Check Point Cluster does not support the Monitor Mode.

Software Blade	Support for the Monitor Mode
Firewall	Fully supports the Monitor Mode.

Software Blade	Support for the Monitor Mode
IPS	<p>These protections and features do not work:</p> <ul style="list-style-type: none"> ▪ The SYN Attack protection (SYNDefender). ▪ The Initial Sequence Number (ISN) Spoofing protection. ▪ The Send error page action in Web Intelligence protections. ▪ Client and Server notifications about connection termination.
Application Control	Does not support UserCheck.
URL Filtering	Does not support UserCheck.
Data Loss Prevention	<p>Does not support these:</p> <ul style="list-style-type: none"> ▪ UserCheck. ▪ The "Prevent" and "Ask User" actions - these are automatically demoted to the "Inform User" action. ▪ FTP inspection.
Identity Awareness	<p>Does not support these:</p> <ul style="list-style-type: none"> ▪ Captive Portal. ▪ Identity Agent.
Threat Emulation	<p>Does not support these:</p> <ul style="list-style-type: none"> ▪ The Emulation Connection Prevent Handling Modes "Background" and "Hold". See sk106119. ▪ FTP inspection.
Content Awareness	Does not support the FTP inspection.
Anti-Bot	Fully supports the Monitor Mode.
Anti-Virus	Does not support the FTP inspection.
IPsec VPN	Does not support the Monitor Mode.
Mobile Access	Does not support the Monitor Mode.
Anti-Spam & Email Security	Does not support the Monitor Mode.
QoS	Does not support the Monitor Mode.

Limitations in Monitor Mode

These features and deployments are **not** supported in Monitor Mode:

- Passing production traffic through a Security Gateway, on which you configured Monitor Mode interface(s).
- If you configure more than one Monitor Mode interface on a Security Gateway, you must make sure the Security Gateway does not receive the same traffic on the different Monitor Mode interfaces.
- HTTPS Inspection
- NAT rules.
- HTTP / HTTPS proxy.
- Anti-Virus in Traditional Mode.
- User Authentication.
- Client Authentication.
- Check Point Active Streaming (CPAS).
- Cluster deployment.
- CloudGuard Gateways.
- CoreXL Dynamic Dispatcher ([sk105261](#)).
- Setting the value of the kernel parameters "psl_tap_enable" and "fw_tap_enable" to 1 (one) on-the-fly with the "fw ctl set int" command (Issue ID 02386641).

For more information, see [sk101670: Monitor Mode on Gaia OS and SecurePlatform OS](#).

Configuring a 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Management Connection window, select the interface, through which you connect to Gaia operating system. ▪ In the Internet Connection window, do not configure IP addresses. ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, clear Unit is a part of a cluster, type. ▪ In the Dynamically Assigned IP window, select No. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).

2. Configure the Monitor Mode on the applicable interface

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia 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: 5px 0;"> <code>https://<IP address of Gaia Management Interface></code> </div> <p>If you changed the default port of Gaia Portal from 443, then you must also enter it (<code>https://<IP address>:<Port></code>).</p>
2	<p>In the left navigation tree, click Network Management > Network Interfaces.</p>
3	<p>Select the applicable physical interface from the list and click Edit.</p>
4	<p>Select the Enable option to set the interface status to UP.</p>
5	<p>In the Comment field, enter the applicable comment text (up to 100 characters).</p>
6	<p>On the IPv4 tab, select Use the following IPv4 address, but do not enter an IPv4 address.</p>
7	<p>On the IPv6 tab, select Use the following IPv6 address, but do not enter an IPv6 address.</p> <p> Important - This setting is available only after you enable the IPv6 Support in Gaia and reboot.</p>
8	<p>On the Ethernet tab:</p> <ul style="list-style-type: none"> ▪ Select Auto Negotiation, or select a link speed and duplex setting from the list. ▪ In the Hardware Address field, enter the Hardware MAC address (if not automatically received from the NIC). <ul style="list-style-type: none">  Caution - Do not manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure. ▪ In the MTU field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ▪ Select Monitor Mode.
9	<p>Click OK.</p>

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>show interface <Name of Physical Interface></pre>
4	If the applicable physical interface has an IP address assigned to it, remove that IP address. <ul style="list-style-type: none"> ■ To remove an IPv4 address: <pre>delete interface <Name of Physical Interface> ipv4-address</pre> ■ To remove an IPv6 address: <pre>delete interface <Name of Physical Interface> ipv6-address</pre>
5	Enable the Monitor Mode on the physical interface: <pre>set interface <Name of Physical Interface> monitor-mode on</pre>
6	Configure other applicable settings on the interface in the Monitor Mode: <pre>set interface <Name of Physical Interface> ...</pre>
7	Examine the configuration and state of the Monitor Mode interface: <pre>show interface <Name of Physical Interface></pre>
8	Save the configuration: <pre>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	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 Gateways & Servers .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click the New (*) > Gateway. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > New Gateway. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Gateway.
4	In the Check Point Security Gateway Creation window, click Wizard Mode .
5	<p>On the General Properties page:</p> <ol style="list-style-type: none"> a. In the Gateway name field, enter the applicable name for this Security Gateway object. b. In the Gateway platform field, select the correct hardware type. c. In the Gateway IP address section, select Static IP address and configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Security Gateway's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses. d. Click Next.
6	<p>On the Trusted Communication page:</p> <ol style="list-style-type: none"> a. Select the applicable option: <ul style="list-style-type: none"> ▪ If you selected Initiate trusted communication now, enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. ▪ If you selected Skip and initiate trusted communication later, make sure to follow Step 7. b. Click Next.



Step	Instructions
7	<p>On the End page:</p> <ol style="list-style-type: none"> Examine the Configuration Summary. Select Edit Gateway properties for further configuration. Click Finish. <p>Check Point Gateway properties window opens on the General Properties page.</p>
8	<p>If during the Wizard Mode, you selected Skip and initiate trusted communication later:</p> <ol style="list-style-type: none"> The Secure Internal Communication field shows Uninitialized. Click Communication. In the Platform field: <ul style="list-style-type: none"> ▪ Select Open server / Appliance for all Check Point models 3000 and higher. ▪ Select Open server / Appliance for an Open Server. Enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. Click Initialize. Make sure the Certificate state field shows Established. Click OK.
9	<p>On the Network Security tab, make sure to enable only the Firewall Software Blade.</p>
10	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Click Get Interfaces > Get Interfaces With Topology. Confirm the interfaces information.

Step	Instructions
11	<p>Select the interface in the Monitor Mode and click Edit.</p> <p>Configure these settings:</p> <ol style="list-style-type: none"> Click the General page. In the General section, enter a <i>random</i> IPv4 address. <ul style="list-style-type: none">  Important - This random IPv4 address must not conflict with existing IPv4 addresses on your network. In the Topology section: <ul style="list-style-type: none"> Click Modify. In the Leads To section, select Not defined (Internal). In the Security Zone section, select According to topology: Internal Zone. Click OK to close the Topology Settings window. Click OK to close the Interface window.
12	Click OK .
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 Gateways & Servers .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> From the top toolbar, click the New (*) > Gateway. In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > New Gateway. In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Gateway.
4	<p>In the Check Point Security Gateway Creation window, click Classic Mode.</p> <p>Check Point Gateway properties window opens on the General Properties page.</p>

Step	Instructions
5	In the Name field, enter the applicable name for this Security Gateway object.
6	<p>In the IPv4 address and IPv6 address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Security 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>
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:</p> <ol style="list-style-type: none"> Near the Secure Internal Communication field, click Communication. In the Platform field: <ul style="list-style-type: none"> Select Open server / Appliance for all Check Point models 3000 and higher. Select Open server / Appliance for an Open Server. Enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. Click Initialize. Click OK.
	<p>If the Certificate state field does not show <code>Established</code>, perform these steps:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Gateway. Make sure there is a physical connectivity between the Security Gateway and the Management Server (for example, pings can pass). Run: <div data-bbox="549 1438 1458 1503" style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>cpconfig</code></div> Enter the number of this option: <div data-bbox="549 1550 1458 1615" style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>Secure Internal Communication</code></div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.

Step	Instructions
8	<p>In the Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: <ul style="list-style-type: none"> If you install the Security Gateway on a Check Point Appliance, select the correct appliances series. If you install the Security Gateway on an Open Server, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
9	<p>On the Network Security tab, make sure to enable only the Firewall Software Blade.</p> <p> Important - Do not select anything on the Management tab.</p>
10	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Click Get Interfaces > Get Interfaces With Topology. Confirm the interfaces information.
11	<p>Select the interface in the Monitor Mode and click Edit. Configure these settings:</p> <ol style="list-style-type: none"> Click the General page. In the General section, enter a <i>random</i> IPv4 address. <p> Important - This random IPv4 address must not conflict with existing IPv4 addresses on your network.</p> In the Topology section: Click Modify. In the Leads To section, select Not defined (Internal). In the Security Zone section, select According to topology: Internal Zone. Click OK to close the Topology Settings window. Click OK to close the Interface window.
12	Click OK .
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.
3	<p>Modify the <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <p>a. Back up the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre data-bbox="512 510 1401 609">cp -v \$FWDIR/boot/modules/fwkernel.conf{, _BKP}</pre> <p>If this file does not exist, create it:</p> <pre data-bbox="512 660 1401 721">touch \$FWDIR/boot/modules/fwkernel.conf</pre> <p>b. Edit the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre data-bbox="512 772 1401 833">vi \$FWDIR/boot/modules/fwkernel.conf</pre> <p> Important - This configuration file does not support spaces or comments.</p> <p>c. Add this line to enable the Passive Streaming Layer (PSL) Tap Mode:</p> <pre data-bbox="512 1012 1401 1072">psl_tap_enable=1</pre> <p>d. Add this line to enable the Firewall Tap Mode:</p> <pre data-bbox="512 1124 1401 1184">fw_tap_enable=1</pre> <p>e. Save the changes in the file and exit the Vi editor.</p>
4	<p>Modify the <code>\$PPKDIR/conf/simkernel.conf</code> file:</p> <p>a. Back up the current <code>\$PPKDIR/conf/simkernel.conf</code> file:</p> <pre data-bbox="512 1355 1401 1415">cp -v \$PPKDIR/conf/simkernel.conf{, _BKP}</pre> <p>If this file does not exist, create it:</p> <pre data-bbox="512 1467 1401 1527">touch \$PPKDIR/conf/simkernel.conf</pre> <p>b. Edit the current <code>\$PPKDIR/conf/simkernel.conf</code> file:</p> <pre data-bbox="512 1579 1401 1639">vi \$PPKDIR/conf/simkernel.conf</pre> <p> Important - This configuration file does not support spaces or comments.</p> <p>c. Add this line to enable the Firewall Tap Mode:</p> <pre data-bbox="512 1780 1401 1841">fw_tap_enable=1</pre> <p>d. Save the changes in the file and exit the Vi editor.</p>

Step	Instructions
5	Reboot the Security Gateway.
6	<p>Make sure the Security Gateway loaded the new configuration:</p> <p>a. Examine the status of the PSL Tap Mode:</p> <pre>fw ctl get int psl_tap_enable</pre> <p>Output must show: psl_tap_enable = 1</p> <p>b. Examine the status of the Firewall Tap Mode:</p> <pre>fw ctl get int fw_tap_enable</pre> <p>Output must show: fw_tap_enable = 1</p>

i 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</i> Domain Management Server that manages this Security Gateway.
2	In the top left corner, click Menu > Global properties .

Step	Instructions
3	<p>From the left tree, click the Stateful Inspection pane and configure:</p> <ol style="list-style-type: none"> In the Default Session Timeouts section: <ol style="list-style-type: none"> Change the value of the TCP session timeout from the default 3600 to 60 seconds. Change the value of the TCP end timeout from the default 20 to 5 seconds. In the Out of state packets 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).
4	<p>From the left tree, click the Advanced page > click the Configure button, and configure:</p> <ol style="list-style-type: none"> Click FireWall-1 > Stateful Inspection. Clear reject_x11_in_any. Click OK to close the Advanced Configuration window.
5	Click OK to close the Global Properties window.
6	Publish the SmartConsole session.

6. Configure the required Access Control Policy for the Security 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 Security Policies .
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> At the top, click the + tab (or press the CTRL T keys). On the Manage Policies tab, click Manage policies and layers. In the Manage policies and layers window, create a new policy and configure the applicable layers. Click Close. On the Manage Policies tab, click the new policy you created.

Step	Instructions																		
4	<p>Create the Access Control 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 & Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Accept All</td> <td>*Any</td> <td>*Any</td> <td>Any</td> <td>*Any</td> <td>Accept</td> <td>Log</td> <td>Object of Security Gateway in Monitor Mode</td> </tr> </tbody> </table>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On	1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On											
1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode											
5	<p> Best Practice</p> <p>We recommend these Aggressive Aging settings for the most common TCP connections:</p> <ol style="list-style-type: none"> In the SmartConsole, click Objects menu > Object Explorer. Open Services and select TCP. Search for the most common TCP connections in this network. Double-click the applicable TCP service. From the left tree, click Advanced. At the top, select Override default settings. On Domain Management Server, select Override global domain settings. Select Match for 'Any'. In the Aggressive aging section: Select Enable aggressive aging. Select Specific and enter 60. Click OK. Close the Object Explorer. 																		
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.

Step	Instructions
2	Log in to the Expert mode.
3	Install the default policy on the VSX Gateway object: Make sure the parameter fw_span_port_mode is part of the installed policy: <pre data-bbox="432 434 1458 539">grep -A 3 -r fw_span_port_mode \$FWDIR/state/local/*</pre> The returned output must show: <pre data-bbox="432 584 1458 647">: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:

- [R81.20 Gaia Administration Guide](#).
- [R81.20 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Management Connection window, select the interface, through which you connect to Gaia operating system. ▪ In the Internet Connection window, do not configure IP addresses. ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, clear Unit is a part of a cluster, type. ▪ In the Dynamically Assigned IP window, select No. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).

2. Configure the Monitor Mode on the applicable interface

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia 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: 5px; margin: 5px 0;"> <code>https://<IP address of Gaia Management Interface></code> </div> If you changed the default port of Gaia Portal from 443, then you must also enter it (<code>https://<IP address>:<Port></code>).
2	In the left navigation tree, click Network Management > Network Interfaces .
3	Select the applicable physical interface from the list and click Edit .
4	Select the Enable option to set the interface status to UP.
5	In the Comment field, enter the applicable comment text (up to 100 characters).
6	On the IPv4 tab, select Use the following IPv4 address , but do not enter an IPv4 address.
7	On the IPv6 tab, select Use the following IPv6 address , but do not enter an IPv6 address.  Important - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the Ethernet tab: <ul style="list-style-type: none"> ▪ Select Auto Negotiation, or select a link speed and duplex setting from the list. ▪ In the Hardware Address field, enter the Hardware MAC address (if not automatically received from the NIC). <ul style="list-style-type: none">  Caution - Do not manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure. ▪ In the MTU field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ▪ Select Monitor Mode.
9	Click OK .

Configuring the Monitor Mode in Gaia 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>show interface <Name of Physical Interface></pre>
4	If the applicable physical interface has an IP address assigned to it, remove that IP address. <ul style="list-style-type: none"> To remove an IPv4 address: <pre>delete interface <Name of Physical Interface> ipv4-address</pre> To remove an IPv6 address: <pre>delete interface <Name of Physical Interface> ipv6-address</pre>
5	Enable the Monitor Mode on the physical interface: <pre>set interface <Name of Physical Interface> monitor-mode on</pre>
6	Configure other applicable settings on the interface in the Monitor Mode: <pre>set interface <Name of Physical Interface> ...</pre>
7	Examine the configuration and state of the Monitor Mode interface: <pre>show interface <Name of Physical Interface></pre>
8	Save the configuration: <pre>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.

Step	Instructions
2	Log in to the Expert mode.
3	<p>Modify the <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <ol style="list-style-type: none"> Back up the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file: <pre>cp -v \$FWDIR/boot/modules/fwkernel.conf{, _BKP}</pre> <p>If this file does not exist, create it:</p> <pre>touch \$FWDIR/boot/modules/fwkernel.conf</pre> Edit the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file: <pre>vi \$FWDIR/boot/modules/fwkernel.conf</pre> <p>Important - This configuration file does not support spaces or comments.</p> Add this line to enable the Passive Streaming Layer (PSL) Tap Mode: <pre>psl_tap_enable=1</pre> Add this line to enable the Firewall Tap Mode: <pre>fw_tap_enable=1</pre> Save the changes in the file and exit the Vi editor.
4	<p>Modify the <code>\$PPKDIR/conf/simkernel.conf</code> file:</p> <ol style="list-style-type: none"> Back up the current <code>\$PPKDIR/conf/simkernel.conf</code> file: <pre>cp -v \$PPKDIR/conf/simkernel.conf{, _BKP}</pre> <p>If this file does not exist, create it:</p> <pre>touch \$PPKDIR/conf/simkernel.conf</pre> Edit the current <code>\$PPKDIR/conf/simkernel.conf</code> file: <pre>vi \$PPKDIR/conf/simkernel.conf</pre> <p>Important - This configuration file does not support spaces or comments.</p> Add this line to enable the Firewall Tap Mode: <pre>fw_tap_enable=1</pre> Save the changes in the file and exit the Vi editor.
5	Reboot the VSX Gateway.

Step	Instructions
6	<p>Make sure the VSX Gateway loaded the new configuration:</p> <p>a. Examine the status of the PSL Tap Mode:</p> <pre>fw ctl get int psl_tap_enable</pre> <p>Output must show: psl_tap_enable = 1</p> <p>b. Examine the status of the Firewall Tap Mode:</p> <pre>fw ctl get int fw_tap_enable</pre> <p>Output must show: fw_tap_enable = 1</p>


i **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 Domain Management Server</i> that should manage this VSX Gateway.
2	From the left navigation panel, click Gateways & Servers .
3	<p>Create a new VSX Gateway object in one of these ways:</p> <ul style="list-style-type: none"> ■ From the top toolbar, click the New (*) > VSX > Gateway. ■ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > VSX > New Gateway. ■ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > VSX > Gateway. <p>The VSX Gateway Wizard opens.</p>

Step	Instructions
4	<p>On the VSX Gateway General Properties (Specify the object's basic settings) page:</p> <ol style="list-style-type: none"> In the Enter the VSX Gateway Name field, enter the applicable name for this VSX Gateway object. In the Enter the VSX Gateway IPv4 field, enter the same IPv4 address that you configured on the Management Connection page of the VSX Gateway's First Time Configuration Wizard. In the Enter the VSX Gateway IPv6 field, enter the same IPv6 address that you configured on the Management Connection page of the VSX Gateway's First Time Configuration Wizard. In the Select the VSX Gateway Version field, select R81.20. Click Next.
5	<p>On the VSX Gateway General Properties (Secure Internal Communication) page:</p> <ol style="list-style-type: none"> In the Activation Key field, enter the same Activation Key you entered during the VSX Gateway's First Time Configuration Wizard. In the Confirm Activation Key field, enter the same Activation Key again. Click Initialize. Click Next.
	<p>If the Trust State field does not show Trust established, perform these steps:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Make sure there is a physical connectivity between the VSX Gateway and the Management Server (for example, pings can pass). Run: <div data-bbox="512 1406 1460 1473" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> Enter the number of this option: <div data-bbox="512 1518 1460 1585" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, on the VSX Gateway General Properties page, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.

Step	Instructions
6	<p>On the VSX Gateway Interfaces (Physical Interfaces Usage) page:</p> <ol style="list-style-type: none"> Examine the list of the interfaces - it must show all the physical interfaces on the VSX Gateway. If you plan to connect more than one Virtual System directly to the same physical interface, you must select VLAN Trunk for that physical interface. Click Next.
7	<p>On the Virtual Network Device Configuration (Specify the object's basic settings) page:</p> <ol style="list-style-type: none"> You can select Create a Virtual Network Device and configure the first applicable Virtual Network Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. Click Next.
8	<p>On the VSX Gateway Management (Specify the management access rules) page:</p> <ol style="list-style-type: none"> Examine the default access rules. Select the applicable default access rules. Configure the applicable source objects, if needed. Click Next. <p> Important - 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 VSX Gateway Creation Finalization page:</p> <ol style="list-style-type: none"> Click Finish and wait for the operation to finish. Click View Report for more information. Click Close.
10	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <div data-bbox="509 1608 1458 1671" style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>vsx stat -v</pre> </div>

Step	Instructions
11	<p>Install the default policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the default policy for this VSX Gateway object. This policy is called: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"> <code><Name of VSX Gateway object>_VSX</code> </div> Click Install.
12	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"> <code>vsx stat -v</code> </div>

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>
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 IPv4 Configuration section, enter a <i>random</i> IPv4 address.</p> <p> Important - 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"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <div style="border: 1px solid black; padding: 2px; width: fit-content; margin: 5px 0;"> <code>vsx stat -v</code> </div>

Step	Instructions
4	<p>Disable the Anti-Spoofing on the interface that is configured in the Monitor Mode:</p> <ol style="list-style-type: none"> In the SmartConsole, open the Virtual System object. Click the Topology page. Select the Monitor Mode interface and click Edit. The Interface Properties window opens. Click the General tab. In the Security Zone field, select None. Click the Topology tab. In the Topology section, make sure the settings are Internal (leads to the local network) and Not Defined. In the Anti-Spoofing section, clear Perform Anti-Spoofing based on interface topology. Click OK to close the Interface Properties window. Click OK to close the Virtual System Properties window. The Management Server pushes the VSX Configuration.


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</i> Domain Management Server that manages this Virtual System.
2	In the top left corner, click Menu > Global properties .
3	<p>From the left tree, click the Stateful Inspection pane and configure:</p> <ol style="list-style-type: none"> In the Default Session Timeouts section: <ol style="list-style-type: none"> Change the value of the TCP session timeout from the default 3600 to 60 seconds. Change the value of the TCP end timeout from the default 20 to 5 seconds. In the Out of state packets 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).
4	<p>From the left tree, click the Advanced page > click the Configure button, and configure:</p> <ol style="list-style-type: none"> Click FireWall-1 > Stateful Inspection. Clear reject_x11_in_any. Click OK to close the Advanced Configuration window.

Step	Instructions
5	Click OK to close the Global Properties window.
6	Publish the SmartConsole session.

7. Configure the required Access Control policy for the Virtual System in SmartConsole

Step	Instructions																		
1	Connect with SmartConsole to the Security Management Server or <i>Target Domain Management Server</i> that manages this Virtual System.																		
2	From the left navigation panel, click Security Policies .																		
3	Create a new policy and configure the applicable layers: <ol style="list-style-type: none"> At the top, click the + tab (or press the CTRL T keys). On the Manage Policies tab, click Manage policies and layers. In the Manage policies and layers window, create a new policy and configure the applicable layers. Click Close. On the Manage Policies tab, click the new policy you created. 																		
4	Create the Access Control rule that accepts all traffic: <table border="1" data-bbox="379 1151 1460 1487"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services & Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </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 On	1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Virtual System
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On											
1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Virtual System											

Step	Instructions
5	<p> Best Practice</p> <p>We recommend these Aggressive Aging settings for the most common TCP connections:</p> <ol style="list-style-type: none"> In the SmartConsole, click Objects menu > Object Explorer. Open Services and select TCP. Search for the most common TCP connections in this network. Double-click the applicable TCP service. From the left tree, click Advanced. At the top, select Override default settings. On Domain Management Server, select Override global domain settings. Select Match for 'Any'. In the Aggressive aging section: <ul style="list-style-type: none"> Select Enable aggressive aging. Select Specific and enter 60. Click OK. Close the Object Explorer.
6	Publish the SmartConsole session.
7	<p>Install the Access Control Policy on the Virtual System object.</p> <ol style="list-style-type: none"> Click Install Policy. In the Policy field, select the applicable policy for this Virtual System object. Click Install.
8	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> Connect to the command line on the VSX Gateway. Log in to the Expert mode. Run: <div data-bbox="464 1543 1458 1608" style="border: 1px solid gray; padding: 5px; margin-top: 5px;"> <pre>vsx stat -v</pre> </div>

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.

Step	Instructions
3	<p data-bbox="427 237 1404 353">Install the default policy on the VSX Gateway object: Make sure the parameter fw_span_port_mode is part of the installed policy:</p> <pre data-bbox="427 360 1461 465">grep -A 3 -r fw_span_port_mode \$FWDIR/state/local/*</pre> <p data-bbox="427 472 877 504">The returned output must show:</p> <pre data-bbox="427 510 1461 577">: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:

- [R81.20 Gaia Administration Guide](#).
- [R81.20 VSX Administration Guide](#).
- [R81.20 Security Management Administration Guide](#).

Configuring Specific Software Blades for Monitor Mode


This section shows how to configure specific Software Blades for Monitor Mode.

 **Note** - For VSX, see:

- [sk79700: VSX supported features on R75.40VS and above](#)
- [sk106496: Software Blades updates on VSX R75.40VS and above - FAQ](#)

Configuring the Threat Prevention Software Blades for Monitor Mode

Configure the settings below, if you enabled one of the Threat Prevention Software Blades (IPS, Anti-Bot, Anti-Virus, Threat Emulation or Threat Extraction) on the Security 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 Security Policies > Threat Prevention .								
3	<p>Create the Threat Prevention rule that accepts all traffic:</p> <table border="1"> <thead> <tr> <th>Protected Scope</th> <th>Protection/Site/File/Blade</th> <th>Action</th> <th>Track</th> </tr> </thead> <tbody> <tr> <td>*Any</td> <td>-- N/A</td> <td>Applicable Threat Prevention Profile</td> <td>Log Packet Capture</td> </tr> </tbody> </table> <p> Notes:</p> <ul style="list-style-type: none"> ▪ We recommend the Optimized profile. ▪ The Track setting Packet Capture is optional. 	Protected Scope	Protection/Site/File/Blade	Action	Track	*Any	-- N/A	Applicable Threat Prevention Profile	Log Packet Capture
Protected Scope	Protection/Site/File/Blade	Action	Track						
*Any	-- N/A	Applicable Threat Prevention Profile	Log Packet Capture						
4	Right-click the selected Threat Prevention profile and click Edit .								
5	<p>From the left tree, click the General Policy page and configure:</p> <ol style="list-style-type: none"> a. In the Blades Activation section, select the applicable Software Blades. b. In the Activation Mode section: <ul style="list-style-type: none"> ▪ In the High Confidence field, select Detect. ▪ In the Medium Confidence field, select Detect. ▪ In the Low Confidence field, select Detect. 								
6	<p>From the left tree, click the Anti-Virus page and configure:</p> <ol style="list-style-type: none"> a. In the Protected Scope section, select Inspect incoming and outgoing files. b. In the File Types section: <ul style="list-style-type: none"> ▪ Select Process all file types. ▪ Optional: Select Enable deep inspection scanning (impacts performance). c. Optional: In the Archives section, select Enable Archive scanning (impacts performance). 								

Step	Instructions
7	From the left tree, click the Threat Emulation page > click General and configure: <ul style="list-style-type: none"><li data-bbox="357 286 1394 360">▪ In the Protected Scope section, select Inspect incoming files from the following interfaces and from the menu, select All.
8	Configure other applicable settings for the Software Blades.
9	Click OK .
10	Install the Threat Prevention Policy on the Security Gateway object.

For more information:

See the [R81.20 Threat Prevention Administration Guide](#).

Configuring the Application Control and URL Filtering Software Blades for Monitor Mode

Configure the settings below, if you enabled Application Control or URL Filtering Software Blade on the Security 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 Manage & Settings > Blades .
3	In the Application Control & URL Filtering section, click Advanced Settings . The Application Control & URL Filtering Settings window opens.
4	On the General page: <ul style="list-style-type: none"> ▪ In the Fail mode section, select Allow all requests (fail-open). ▪ In the URL Filtering section, select Categorize HTTPS websites.
5	On the Check Point online web service page: <ul style="list-style-type: none"> ▪ In the Website categorization mode section, select Background. ▪ Select Categorize social networking widgets.
6	Click OK to close the Application Control & URL Filtering Settings window.
7	Install the Access Control Policy on the Security Gateway object.

For more information, see the:

- [R81.20 Security Management Administration Guide](#).
- [R81.20 Quantum 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 Manage & Settings > Blades .
3	In the Data Loss Prevention section, click Configure in SmartDashboard . The SmartDashboard window opens.
4	<p>In SmartDashboard:</p> <ol style="list-style-type: none"> Click the My Organization page. In the Email Addresses or Domains section, configure with full list of company's domains. There is no need to include subdomains (for example, <code>mydomain.com</code>, <code>mydomain.uk</code>). In the Networks section, select Anything behind the internal interfaces of my DLP gateways. In the Users section, select All users.
5	<p>Click the Policy page. Configure the applicable rules:</p> <ul style="list-style-type: none"> ▪ In the Data column, right-click the pre-defined data types and select Edit. <ul style="list-style-type: none"> • On the General Properties page, in the Flag field, select Improve Accuracy. • In the Customer Names data type, we recommend to add the company's real customer names. ▪ In the Action column, you must select Detect. ▪ In the Severity column, select Critical or High in all applicable rules. ▪ You may choose to disable or delete rules that are not applicable to the company or reduce the Severity of these rules. <p> Note - Before you can configure the DLP rules, you must configure the applicable objects in SmartConsole.</p>

Step	Instructions
6	<p>Click the Additional Settings > Protocols page. Configure these settings:</p> <ul style="list-style-type: none"> ▪ In the Email section, select SMTP (Outgoing Emails). ▪ In the Web section, select HTTP. Do not configure the HTTPS. ▪ In the File Transfer section, do not select FTP.
7	Click Launch Menu > File > Update (or press the CTRL S keys).
8	Close the SmartDashboard.
9	Install the Access Control Policy on the Security Gateway object.
10	<p>Make sure the Security Gateway enabled the SMTP Mirror Port Mode:</p> <ol style="list-style-type: none"> a. Connect to the command line on the Security Gateway. b. Log in to the Expert mode. c. Run this command: <div data-bbox="395 898 1460 965" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>dlp_smtp_mirror_port status</pre> </div> d. Make sure the value of the kernel parameter <code>dlp_force_smtp_kernel_inspection</code> is set to 1 (one). Run these two commands: <div data-bbox="395 1093 1460 1240" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>fw ctl get int dlp_force_smtp_kernel_inspection grep dlp_force_smtp_kernel_inspection \$FWDIR/boot/modules/fwkern.conf</pre> </div>

For more information:

See the [R81.20 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 "X Forward-For header". 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 sk100223: How to enable stripping of X-Forward-For (XFF) field .

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 subordinate interfaces, the Security Gateway (or Cluster Members) inspects it and passes it to the second bridge subordinate 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	✓	✓	✓
IPS	✓	✓	✓
URL Filtering	✓	✓	✓
DLP	✓	✓	—
Anti-Bot	✓	✓	✓
Anti-Virus	✓ (1)	✓ (1)	✓ (1)
Application Control	✓	✓	✓
HTTPS Inspection	✓ (2)	✓ (2)	—
Identity Awareness	✓ (3)	✓ (3)	—

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 - ThreatCloud emulation	✓	✓	Yes in Active/Active Bridge Mode No in Active/Standby Bridge Mode
Threat Emulation - Local emulation	✓	✓	No in all Bridge Modes
Threat Emulation - Remote emulation	✓	✓	Yes in Active/Active Bridge Mode No in Active/Standby Bridge Mode
Threat Extraction	✓	✓	Yes in Active/Active Bridge Mode No in Active/Standby Bridge Mode
Zero Phishing	–	–	–
UserCheck	✓	✓	–
QoS	✓ (see sk89581)	– (see sk89581)	– (see sk79700)
HTTP / HTTPS proxy	✓	✓	–
Security Servers - SMTP, HTTP, FTP, POP3	✓	✓	–
Client Authentication	✓	✓	–
User Authentication	✓	✓	–

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
Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on)	✓	–	–
IPsec VPN	–	–	–
Mobile Access	–	–	–

 **Notes:**

- Does not support the Anti-Virus in Traditional Mode.
- HTTPS Inspection in Layer 2 works as Man-in-the-Middle, based on MAC addresses:
 - Client sends a TCP [SYN] packet to the MAC address X.
 - Security Gateway creates a TCP [SYN-ACK] packet and sends it to the MAC address X.
 - Security Gateway in Bridge Mode does not need IP addresses, because CPAS takes the routing and the MAC address from the original packet.

Note - To be able to perform certificate validation (CRL/OCSP download), Security Gateway needs at least one interface to be assigned with an IP address. Probe bypass can have issues with Bridge Mode. Therefore, we do not recommend Probe bypass in Bridge Mode configuration.
- Identity Awareness in Bridge Mode supports only the AD Query authentication.

Limitations in Bridge Mode

You can configure only **two** subordinate 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.

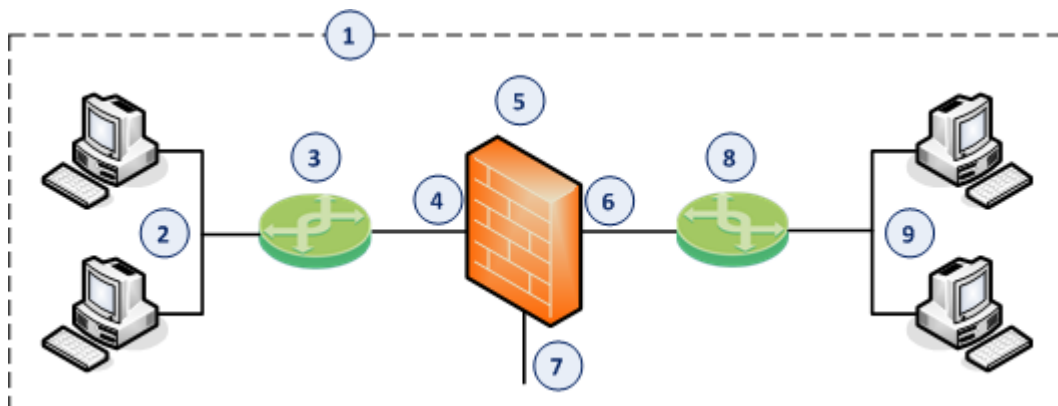
(Asymmetric traffic inspection is any situation, where the Client-to-Server packet is inspected by one Cluster Member, while the Server-to-Client packet is inspected by the other Cluster Member. In such scenarios, several security features do not work.)

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 subordinate interface (4) on the Security Gateway in Bridge Mode.
4	One bridged subordinate interface (for example, <code>eth1</code>) on the Security Gateway in Bridge Mode.
5	Security Gateway in Bridge Mode.
6	Another bridged subordinate 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 subordinate 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Management Connection window, select the interface, through which you connect to Gaia operating system. ▪ In the Internet Connection window, do not configure IP addresses. ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, clear Unit is a part of a cluster, type. ▪ In the Dynamically Assigned IP window, select No. ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).

2. Configure the Bridge interface on the Security Gateway

You configure the Bridge interface in either Gaia Portal, or Gaia Clish.

Configuring the Bridge interface in Gaia Portal

 **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.


Step	Instructions
1	In the left navigation tree, click Network Management > Network Interfaces .
2	Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned.

Step	Instructions
3	Click Add > Bridge . To configure an existing Bridge interface, select the Bridge interface and click Edit .
4	On the Bridge tab, enter or select a Bridge Group ID (unique integer between 1 and 1024).
5	Select the interfaces from the Available Interfaces list and then click Add . i Notes: <ul style="list-style-type: none"> ▪ Make sure that the subordinate interfaces do not have any IP addresses or aliases configured. ▪ Do not select the interface that you configured as Gaia Management Interface. ▪ A Bridge interface in Gaia can contain only two subordinate interfaces.
6	On the IPv4 tab, enter the IPv4 address and subnet mask. You can optionally select the Obtain IPv4 Address automatically option.
7	On the IPv6 tab (optional), enter the IPv6 address and mask length. You can optionally select the Obtain IPv6 Address automatically option. i Important - First, you must enable the IPv6 Support and reboot.
8	Click OK .

i **Notes:**

- 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*".
- To configure MTU on a Bridge subordinate interface, you must configure MTU on the Bridge interface.
This MTU applies to all subordinate interfaces assigned to this Bridge interface.

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	<p>Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:</p> <pre data-bbox="467 526 1460 629">show interface <Name of Interface> ipv4-address show interface <Name of Interface> ipv6-address</pre>
4	<p>Add a new bridging group:</p> <pre data-bbox="467 712 1460 775">add bridging group <Bridge Group ID 0 - 1024></pre>
5	<p>Add subordinate interfaces to the new bridging group:</p> <pre data-bbox="467 857 1460 1037">add bridging group <Bridge Group ID> interface <Name of First Subordinate Interface> add bridging group <Bridge Group ID> interface <Name of Second Subordinate Interface></pre> <p> Notes:</p> <ul style="list-style-type: none"> ▪ Do not select the interface that you configured as Gaia Management Interface. ▪ A Bridge interface in Gaia can contain only two subordinate interfaces.

Step	Instructions
6	<p>Assign an IP address to the bridging group.</p> <ul style="list-style-type: none"> To assign an IPv4 address, run: <pre>set interface <Name of Bridge Interface> ipv4-address <IPv4 Address> {subnet-mask <Mask> mask-length <Mask Length>}</pre> <p>You can optionally configure the bridging group to obtain an IPv4 Address automatically.</p> To assign an IPv6 address, run: <pre>set interface <Name of Bridge Interface> ipv6-address <IPv6 Address> mask-length <Mask Length></pre> <p>You can optionally configure the bridging group to obtain an IPv6 Address automatically.</p> <p>Important - 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 Gateways & Servers .


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

Step	Instructions
8	<p>If during the Wizard Mode, you selected Skip and initiate trusted communication later:</p> <ol style="list-style-type: none"> The Secure Internal Communication field shows Uninitialized. Click Communication. In the Platform field: <ul style="list-style-type: none"> Select Open server / Appliance for all Check Point models 3000 and higher. Select Open server / Appliance for an Open Server. Enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. Click Initialize. Make sure the Certificate state field shows Established. Click OK.
9	<p>On the General Properties page:</p> <ul style="list-style-type: none"> On the Network Security tab, enable the applicable Software Blades. On the Threat Prevention tab, enable the applicable Software Blades. <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>
10	<p>On the Network Management page, configure the Topology of the Bridge interface.</p> <p> Notes:</p> <ul style="list-style-type: none"> If a Bridge interface connects to the Internet, then set the Topology to External. If you use this Bridge Security Gateway object in Access Control Policy rules with Internet objects, then set the Topology to External.
11	Click OK .
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.


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 Gateways & Servers .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click the New (*) > Gateway. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > New Gateway. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Gateway.
4	<p>In the Check Point Security Gateway Creation window, click Classic Mode.</p> <p>Check Point Gateway properties window opens on the General Properties page.</p>
5	In the Name field, enter the applicable name for this Security Gateway object.
6	<p>In the IPv4 address and IPv6 address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Security 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>
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Gateway:</p> <ol style="list-style-type: none"> a. Near the Secure Internal Communication field, click Communication. b. In the Platform field: <ul style="list-style-type: none"> ▪ Select Open server / Appliance for all Check Point models 3000 and higher. ▪ Select Open server / Appliance for an Open Server. c. Enter the same Activation Key you entered during the Security Gateway's First Time Configuration Wizard. d. Click Initialize. e. Click OK.

Step	Instructions
	<p>If the Certificate state field does not show <code>Established</code>, perform these steps:</p> <ol style="list-style-type: none"> Connect to the command line on the Security Gateway. Make sure there is a physical connectivity between the Security Gateway and the Management Server (for example, pings can pass). Run: <pre>cpconfig</pre> Enter the number of this option: <pre>Secure Internal Communication</pre> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
8	<p>In the Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: <ul style="list-style-type: none"> If you install the Security Gateway on a Check Point Appliance, select the correct appliances series. If you install the Security Gateway on an Open Server, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
9	<p>Enable the applicable Software Blades:</p> <ul style="list-style-type: none"> On the Network Security tab. On the Threat Prevention tab. <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>

Step	Instructions
10	<p>On the Network Management page, configure the Topology of the Bridge interface.</p> <p> Notes:</p> <ul style="list-style-type: none"> ▪ If a Bridge interface connects to the Internet, then set the Topology to External. ▪ If you use this Bridge Security Gateway object in Access Control Policy rules with Internet objects, then set the Topology to External.
11	Click OK .
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

4. Configure the applicable Security Policies for the Security Gateway in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Gateway.
2	From the left navigation panel, click Security Policies .
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> a. At the top, click the + tab (or press CTRL T). b. On the Manage Policies tab, click Manage policies and layers. c. In the Manage policies and layers window, create a new policy and configure the applicable layers. d. Click Close. e. On the Manage Policies tab, click the new policy you created.
4	<p>Create the applicable rules in the Access Control and Threat Prevention policies.</p> <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</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:

- [R81.20 Gaia Administration Guide](#).
- [R81.20 Security Management Administration Guide](#).
- Applicable *Administration Guides* on the [R81.20 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 607](#)
- ["Configuring ClusterXL in Bridge Mode - Active / Active with Two or Four Switches" on page 624](#)

Configuring ClusterXL in Bridge Mode - Active / Standby with Two Switches

Notes:

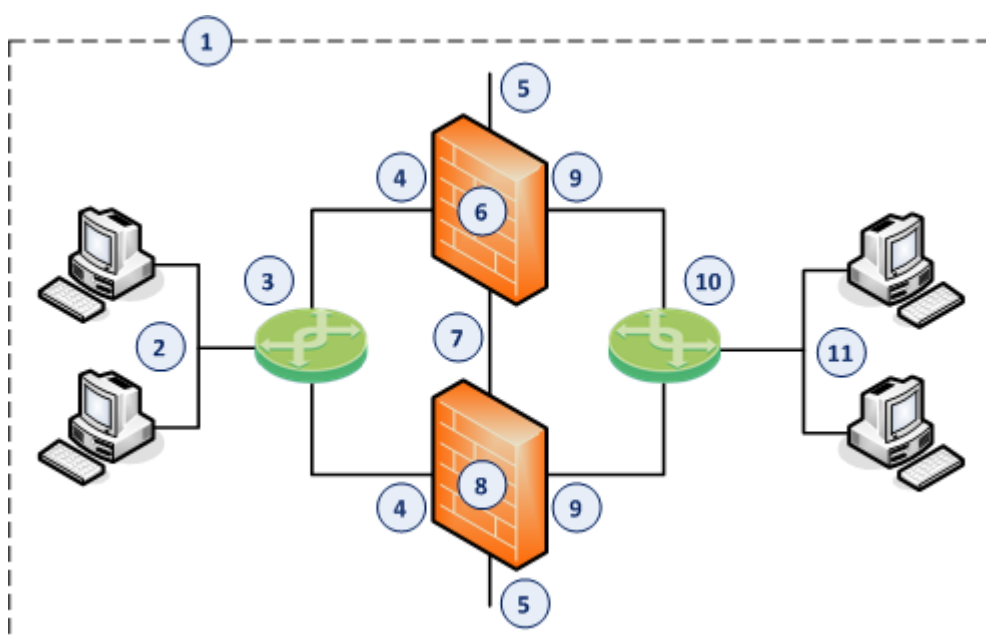
- This procedure applies to both Check Point Appliances and Open Servers.
- ClusterXL deployed in Active/Standby Bridge Mode, supports only two switches.

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 [R81.20 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 subordinate interface (4) on the ClusterXL in Bridge Mode.
4	One bridged subordinate interface (for example, eth1) on the Cluster Members in Bridge Mode.

Item	Instructions
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).
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 subordinate 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 subordinate 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, select these two options: <ul style="list-style-type: none"> • Unit is a part of a cluster • ClusterXL ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).


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 Gateways & Servers .
3	Create a new Cluster object in one of these ways: <ul style="list-style-type: none"> ▪ From the top toolbar, click New (*) > Cluster > Cluster. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.



Step	Instructions
4	In the Check Point Security Gateway Cluster Creation window, click Wizard Mode .
5	<p>On the Cluster General Properties page:</p> <ol style="list-style-type: none"> In the Cluster Name field, enter the applicable name for this ClusterXL object. Configure the main Virtual IP address(es) for this ClusterXL object. In the Cluster IPv4 Address section, enter the main Virtual IPv4 address for this ClusterXL object. In the Cluster IPv6 Address section, enter the main Virtual IPv6 address for this ClusterXL object. In the Choose the Cluster's Solution field, select Check Point ClusterXL and High Availability. Click Next.
6	<p>On the Cluster members' properties page, add the objects for the Cluster Members.</p> <ol style="list-style-type: none"> Click Add > New Cluster Member. The Cluster Member Properties window opens. In the Name field, enter the applicable name for this Cluster Member object. Configure the main physical IP address(es) for this Cluster Member object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.  Note - 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. In the Activation Key and Confirm Activation Key fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard. Click Initialize. Click OK. Repeat Steps a-f to add the second Cluster Member, and so on.


Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="547 524 1460 584" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> Enter the number of this option: <div data-bbox="547 636 1460 696" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
7	<p>On the Cluster Topology page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> Examine the IPv4 Network Address at the top of the page. Select the applicable role: <ul style="list-style-type: none"> ■ For <i>cluster traffic interfaces</i>, select Representing a cluster interface and configure the Cluster Virtual IPv4 address and its Net Mask. <div data-bbox="627 1272 1460 1464" style="margin-left: 20px;"> <p> Note - 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> </div> ■ For <i>cluster synchronization interfaces</i>, select Cluster Synchronization and select Primary only. Check Point cluster supports only one synchronization network. ■ For <i>interfaces that do not pass the traffic between the connected networks</i>, select Private use of each member (don't monitor members interfaces). Click Next

Step	Instructions
8	<p>On the Cluster Definition Wizard Complete page:</p> <ol style="list-style-type: none"> Examine the Configuration Summary. Select Edit Cluster's Properties. Click Finish <p>The Gateway Cluster Properties window opens.</p>
9	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> In the Name field, make sure you see the configured applicable name for this ClusterXL object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
10	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
11	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab. <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>

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


Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="547 524 1460 586" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> Enter the number of this option: <div data-bbox="547 636 1460 698" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
13	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select High Availability and ClusterXL. In the Tracking section, select the applicable option. In the Advanced Settings section: <ol style="list-style-type: none"> Optional: Select Use State Synchronization. <div data-bbox="627 1238 671 1283" style="display: inline-block; vertical-align: middle;">  </div> Best Practice - We recommend to select this option. For more information, click the (?) button in the top right corner. Optional: Select Use Virtual MAC. For more information, see sk50840. Select the Cluster Member recovery method. For more information, click the (?) button in the top right corner.


Step	Instructions
14	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Select each interface and click Edit. The Network: <Name of Interface> window opens. From the left tree, click the General page. In the General section, in the Network Type field, select the applicable type: <ul style="list-style-type: none"> ▪ For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct. ▪ For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync. <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> • We do not recommend the configuration Cluster+Sync. • Check Point cluster supports only these settings: <ul style="list-style-type: none"> ◦ One Sync interface. ◦ One Cluster+Sync interface. ◦ One Sync interface and one Cluster+Sync interface. • For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member. <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> ▪ For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. ▪ 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 R81.20 ClusterXL Administration Guide.


Step	Instructions
	<p>e. In the Topology section:</p> <ul style="list-style-type: none"> ▪ Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> • Override > Network defined by routes (this is the default). • Override > Specific > select the applicable Network object or Network Group object. ▪ To increase the security, enable the Anti-Spoofing. <p> Important:</p> <ul style="list-style-type: none"> ▪ Make sure the Bridge interface and Bridge subordinate interfaces are not in the Topology. ▪ You cannot define the Topology of the Bridge interface. It is External by default.
15	Click OK .
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 Gateways & Servers .
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click New (*) > Cluster > Cluster. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.
4	<p>In the Check Point Security Gateway Creation window, click Classic Mode.</p> <p>The Gateway Cluster Properties window opens.</p>

Step	Instructions
5	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> In the Name field, make sure you see the configured applicable name for this ClusterXL object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
6	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
7	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab. <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>


Step	Instructions
8	<p>On the Cluster Members page:</p> <ol style="list-style-type: none">Click Add > New Cluster Member. The Cluster Member Properties window opens.In the Name field, enter the applicable name for this Cluster Member object.Configure the main physical IP address(es) for this Cluster Member object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.  Note - 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.Click Communication.In the One-time password and Confirm one-time password fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.Click Initialize.Click Close.Click OK.Repeat Steps a-h to add the next Cluster Member.

Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <pre>cpconfig</pre> Enter the number of this option: <pre>Secure Internal Communication</pre> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
9	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select High Availability and ClusterXL. In the Tracking section, select the applicable option. In the Advanced Settings section: <ol style="list-style-type: none"> Optional: Select Use State Synchronization. <ul style="list-style-type: none">  Best Practice - We recommend to select this option. For more information, click the (?) button in the top right corner. Optional: Select Use Virtual MAC. <ul style="list-style-type: none"> For more information, see sk50840. Select the Cluster Member recovery method. <ul style="list-style-type: none"> For more information, click the (?) button in the top right corner.

Step	Instructions
10	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Select each interface and click Edit. The Network: <Name of Interface> window opens. From the left tree, click the General page. In the General section, in the Network Type field, select the applicable type: <ul style="list-style-type: none"> ■ For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct. ■ For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync. <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> • We do not recommend the configuration Cluster+Sync. • Check Point cluster supports only these settings: <ul style="list-style-type: none"> ◦ One Sync interface. ◦ One Cluster+Sync interface. ◦ One Sync interface and one Cluster+Sync interface. • For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface. ■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member. <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> ■ For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. ■ 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 R81.20 ClusterXL Administration Guide.

Step	Instructions
	<p>e. In the Topology section:</p> <ul style="list-style-type: none"> ▪ Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> • Override > Network defined by routes (this is the default). • Override > Specific > select the applicable Network object or Network Group object. ▪ To increase the security, enable the Anti-Spoofing. <p> Important:</p> <ul style="list-style-type: none"> ▪ Make sure the Bridge interface and Bridge subordinate interfaces are not in the Topology. ▪ You cannot define the Topology of the Bridge interface. It is External by default.
11	Click OK .
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 Security Policies .
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> a. At the top, click the + tab (or press CTRL T). b. On the Manage Policies tab, click Manage policies and layers. c. In the Manage policies and layers window, create a new policy and configure the applicable layers. d. Click Close. e. On the Manage Policies tab, click the new policy you created.
4	<p>Create the applicable rules in the Access Control and Threat Prevention policies.</p> <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>

Step	Instructions
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"> In Gaia Clish, run: <pre>show cluster state</pre> In the Expert mode, run: <pre>cphaprob state</pre> <p>Example output:</p> <pre>Member1> 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>
3	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> In Gaia Clish, run: <pre>show cluster members interfaces all</pre> In the Expert mode, run: <pre>cphaprob -a if</pre>

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	<p>Run:</p> <pre>cpconfig</pre>
3	Select Enable Check Point ClusterXL for Bridge Active/Standby .

Item	Instructions
4	Enter y 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	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show cluster state</pre> ■ In the Expert mode, run: <pre>cphaprob state</pre> <p>Example output:</p> <pre>Member1> show cluster state Cluster Mode: High Availability (Active Up, Bridge Mode) 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	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> ■ In Gaia Clish, run: <pre>show cluster members interfaces all</pre> ■ In the Expert mode, run: <pre>cphaprob -a if</pre>

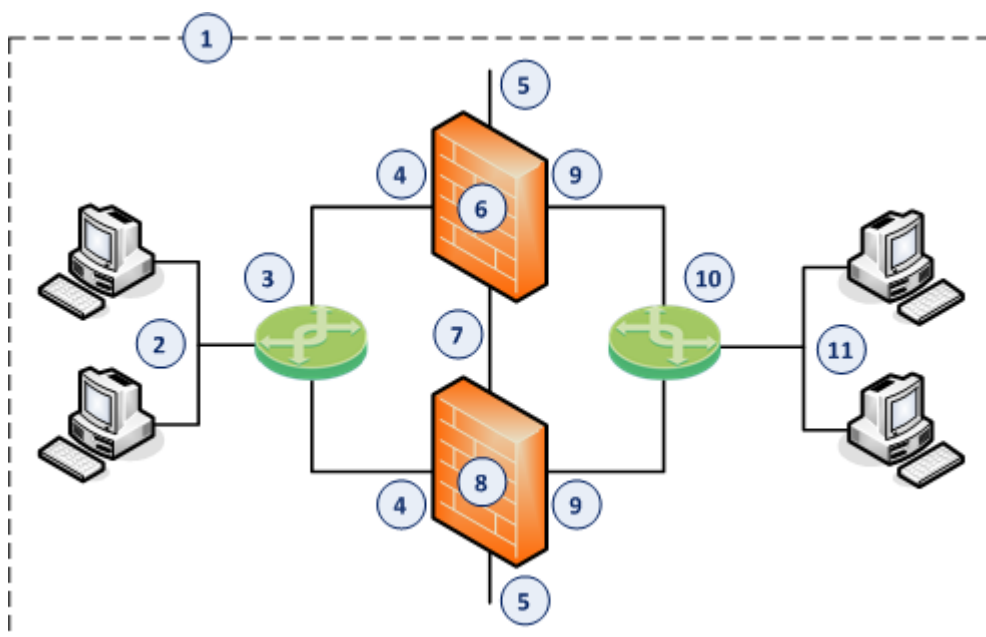
Configuring ClusterXL in Bridge Mode - Active / Active with Two or Four Switches

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.

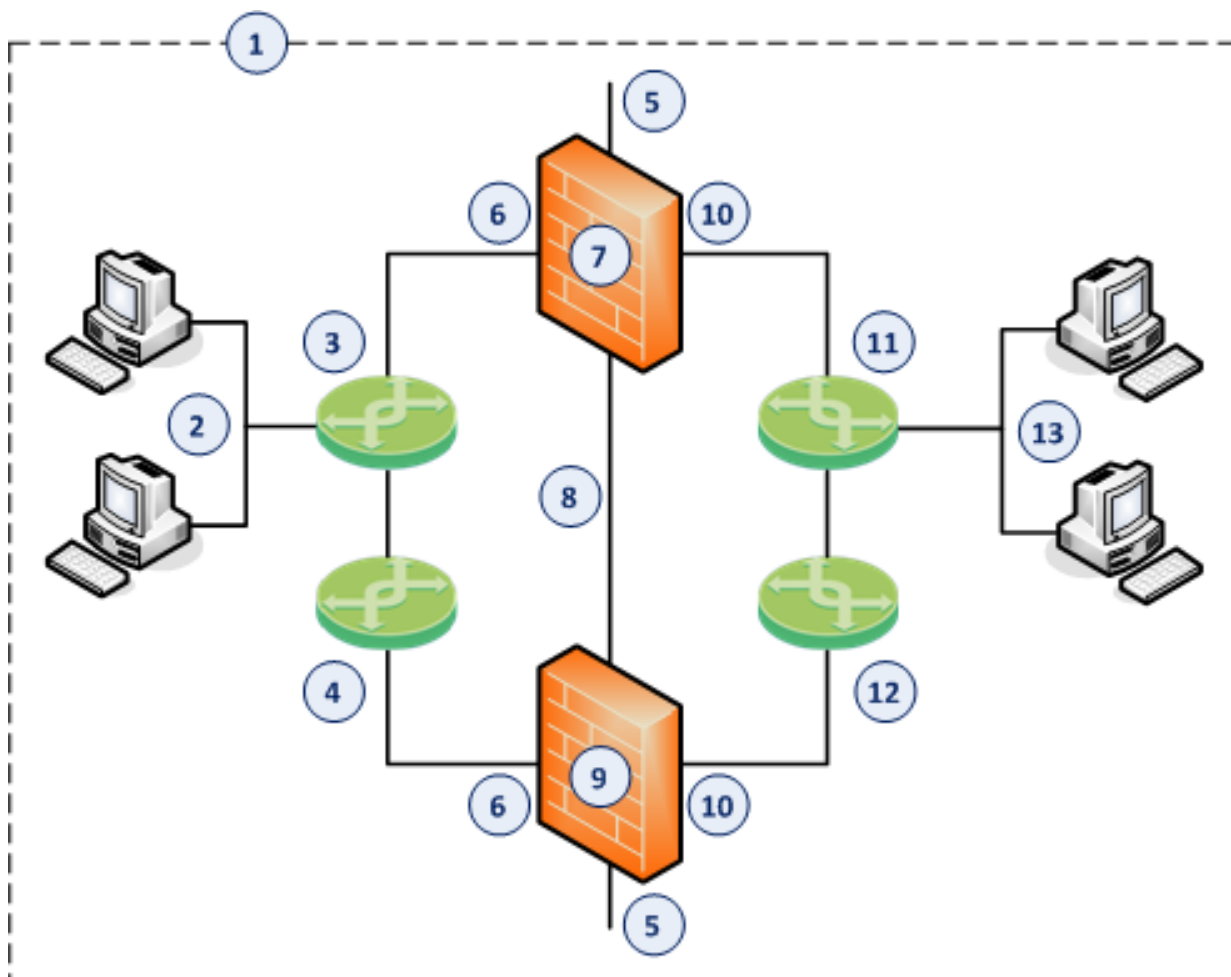
Example Topology with Two Switches



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 subordinate interface (4) on the ClusterXL in Bridge Mode.
4	One bridged subordinate 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.

Item	Instructions
6	First Cluster Member in Bridge Mode (in the <i>Active</i> cluster state).
7	Network that connects dedicated synchronization interfaces (for example, <i>eth3</i>) on the ClusterXL in Bridge Mode.
8	Second Cluster Member in Bridge Mode (in the <i>Active</i> cluster state).
9	Another bridged subordinate interface (for example, <i>eth2</i>) on the Cluster Members in Bridge Mode.
10	Switch that connects the second network segment to the other bridged subordinate 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 subordinate 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 subordinate interface (6) on the ClusterXL in Bridge Mode.
5	Dedicated Gaia Management Interface (for example, <code>eth0</code>) on the Cluster Members.
6	One bridged subordinate interface (for example, <code>eth1</code>) 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, <code>eth3</code>) on the ClusterXL in Bridge Mode.
9	Second Cluster Member in Bridge Mode (in the <code>Active</code> cluster state).
10	Another bridged subordinate interface (for example, <code>eth2</code>) on the Cluster Members in Bridge Mode.
11	Switch that connects the second network segment to the other bridged subordinate 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 subordinate 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"> ▪ "Installing the Gaia Operating System on Check Point Appliances" on page 21 ▪ "Installing the Gaia Operating System on Open Servers" on page 23
2	Follow "Configuring Gaia for the First Time" on page 28 .
3	During the First Time Configuration Wizard, you must configure these settings: <ul style="list-style-type: none"> ▪ In the Installation Type window, select Security Gateway and/or Security Management. ▪ In the Products window: <ol style="list-style-type: none"> a. In the Products section, select Security Gateway only. b. In the Clustering section, select these two options: <ul style="list-style-type: none"> • Unit is a part of a cluster • ClusterXL ▪ In the Secure Internal Communication window, enter the applicable Activation Key (between 4 and 127 characters long).



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

 **Important** - On Scalable Platforms (Maestro and Chassis), you must connect to the Gaia Portal of the applicable Security Group.

Step	Instructions
1	In the left navigation tree, click Network Management > Network Interfaces .
2	Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned.
3	Click Add > Bridge . To configure an existing Bridge interface, select the Bridge interface and click Edit .

Step	Instructions
4	On the Bridge tab, enter or select a Bridge Group ID (unique integer between 1 and 1024).
5	Select the interfaces from the Available Interfaces list and then click Add .  Notes: <ul style="list-style-type: none"> ▪ Make sure that the subordinate interfaces do not have any IP addresses or aliases configured. ▪ Do not select the interface that you configured as Gaia Management Interface. ▪ A Bridge interface in Gaia can contain only two subordinate interfaces.
6	On the IPv4 tab, enter the IPv4 address and subnet mask. You can optionally select the Obtain IPv4 Address automatically option.
7	On the IPv6 tab (optional), enter the IPv6 address and mask length. You can optionally select the Obtain IPv6 Address automatically option.  Important - First, you must enable the IPv6 Support and reboot.
8	Click OK .

 **Notes:**

- 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*".
- To configure MTU on a Bridge subordinate interface, you must configure MTU on the Bridge interface.
This MTU applies to all subordinate interfaces assigned to this Bridge interface.

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.

Step	Instructions
3	<p>Make sure that the subordinate interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:</p> <pre>show interface <Name of Interface> ipv4-address show interface <Name of Interface> ipv6-address</pre>
4	<p>Add a new bridging group:</p> <pre>add bridging group <Bridge Group ID 0 - 1024></pre>
5	<p>Add subordinate interfaces to the new bridging group:</p> <pre>add bridging group <Bridge Group ID> interface <Name of First Subordinate Interface> add bridging group <Bridge Group ID> interface <Name of Second Subordinate Interface></pre> <p>i Notes:</p> <ul style="list-style-type: none"> ▪ A Bridge interface in Gaia can contain only two subordinate interfaces. ▪ Do not select the interface that you configured as Gaia Management Interface.
6	Do not assign an IP address to the bridging group.
7	<p>Save the configuration:</p> <pre>save config</pre>


i **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 Gateways & Servers .

Step	Instructions
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> ■ From the top toolbar, click New (*) > Cluster > Cluster. ■ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. ■ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.
4	<p>In the Check Point Security Gateway Cluster Creation window, click Wizard Mode.</p>
5	<p>On the Cluster General Properties page:</p> <ol style="list-style-type: none"> a. In the Cluster Name field, enter the applicable name for this ClusterXL object. b. Configure the main Virtual IP address(es) for this ClusterXL object. <ul style="list-style-type: none"> ■ In the Cluster IPv4 Address section, enter the main Virtual IPv4 address for this ClusterXL object. ■ In the Cluster IPv6 Address section, enter the main Virtual IPv6 address for this ClusterXL object. <p> Note - 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> c. In the Choose the Cluster's Solution field, select Check Point ClusterXL and select the cluster mode - either High Availability, or Load Sharing. d. Click Next.

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

Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <pre>cpconfig</pre> Enter the number of this option: <pre>Secure Internal Communication</pre> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
7	<p>On the Cluster Topology page, configure the roles of the cluster interfaces:</p> <ol style="list-style-type: none"> Examine the IPv4 Network Address at the top of the page. Select the applicable role: <ul style="list-style-type: none"> ■ For <i>cluster traffic interfaces</i>, select Representing a cluster interface and configure the Cluster Virtual IPv4 address and its Net Mask. <ul style="list-style-type: none">  Note - 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. ■ For <i>cluster synchronization interfaces</i>, select Cluster Synchronization and select Primary only. Check Point cluster supports only one synchronization network. ■ For <i>interfaces that do not pass the traffic between the connected networks</i>, select Private use of each member (don't monitor members interfaces). Click Next

Step	Instructions
8	<p>On the Cluster Definition Wizard Complete page:</p> <ol style="list-style-type: none"> Examine the Configuration Summary. Select Edit Cluster's Properties. Click Finish <p>The Gateway Cluster Properties window opens.</p>
9	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> In the Name field, make sure you see the configured applicable name for this ClusterXL object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
10	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
11	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab. <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>

Step	Instructions
12	<p>On the Cluster Members page:</p> <ol style="list-style-type: none">Click Add > New Cluster Member. The Cluster Member Properties window opens.In the Name field, enter the applicable name for this Cluster Member object.Configure the main physical IP address(es) for this Cluster Member object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.  Note - 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.Click Communication.In the One-time password and Confirm one-time password fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.Click Initialize.Click Close.Click OK.Repeat Steps a-h to add the next Cluster Member.

Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="547 524 1460 589" style="border: 1px solid gray; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> Enter the number of this option: <div data-bbox="547 636 1460 701" style="border: 1px solid gray; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
13	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select the applicable mode: <ul style="list-style-type: none"> ▪ High Availability and ClusterXL ▪ Load Sharing and Multicast or Unicast ▪ Active-Active In the Tracking section, select the applicable option. In the Advanced Settings section:

Step	Instructions
	<ul style="list-style-type: none"> ■ If you selected the High Availability mode, then: <ol style="list-style-type: none"> i. Optional: Select Use State Synchronization. This configures the Cluster Members to synchronize the information about the connections they inspect. <ul style="list-style-type: none"> ★ Best Practice - Enable this setting to prevent connection drops after a cluster failover. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> i Notes: <ul style="list-style-type: none"> • 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 R81.20 ClusterXL Administration Guide. • The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. • The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.



Step	Instructions
	<p>iv. Select the Cluster Member recovery method - which Cluster Member to select as Active during a fallback (return to normal operation after a cluster failover):</p> <ul style="list-style-type: none">• Maintain current active Cluster Member<ol style="list-style-type: none">i. The Cluster Member that is currently in the Active state, remains in this state.ii. Other Cluster Members that return to normal operation, remain in the Standby state.• Switch to higher priority Cluster Member<ol style="list-style-type: none">i. The Cluster Member that has the highest priority (appears at the top of the list on the Cluster Members page of the cluster object) becomes the new Active.ii. The state of the previously Active Cluster Member changes to Standby.iii. Other Cluster Members that return to normal operation remain in the Standby state.


Step	Instructions
	<ul style="list-style-type: none"> ■ If you selected the Load Sharing > Multicast mode, then: <ul style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> 📘 Notes: <ul style="list-style-type: none"> • 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 R81.20 ClusterXL Administration Guide. • The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. • The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Select the connection sharing method between the Cluster Members:

Step	Instructions
	<ul style="list-style-type: none"> <p data-bbox="676 237 938 271">• IPs, Ports, SPIs</p> <p data-bbox="707 280 1458 432">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.</p> <p data-bbox="707 441 1406 551">This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</p> <p data-bbox="707 560 1461 672">This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p data-bbox="707 680 1110 714">We recommend this method.</p> <p data-bbox="676 723 852 757">• IPs, Ports</p> <p data-bbox="707 766 1458 918">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.</p> <p data-bbox="707 927 1458 1001">Use this method only if there are problems when distributing IPsec packets between Cluster Members.</p> <p data-bbox="676 1010 756 1043">• IPs</p> <p data-bbox="707 1052 1458 1205">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.</p> <p data-bbox="707 1214 1406 1323">This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</p> <p data-bbox="707 1332 1461 1444">This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p data-bbox="707 1453 1458 1570">Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>

Step	Instructions
	<ul style="list-style-type: none"> ■ If you selected the Load Sharing > Unicast mode, then: <ol style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> ⓘ Notes: <ul style="list-style-type: none"> • 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 R81.20 ClusterXL Administration Guide. • The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. • The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.


Step	Instructions
	<p>iv. Select the connection sharing method between the Cluster Members:</p> <ul style="list-style-type: none"> <p>• IPs, Ports, SPIs</p> <p>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.</p> <p>This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</p> <p>This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>We recommend this method.</p> <p>• IPs, Ports</p> <p>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.</p> <p>Use this method only if there are problems when distributing IPsec packets between Cluster Members.</p> <p>• IPs</p> <p>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.</p> <p>This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</p> <p>This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>


Step	Instructions
14	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Select each interface and click Edit. The Network: <Name of Interface> window opens. From the left tree, click the General page. In the General section, in the Network Type field, select the applicable type: <ul style="list-style-type: none"> ▪ For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct. ▪ For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync. <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> • We do not recommend the configuration Cluster+Sync. • Check Point cluster supports only these settings: <ul style="list-style-type: none"> ◦ One Sync interface. ◦ One Cluster+Sync interface. ◦ One Sync interface and one Cluster+Sync interface. • For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member. <ul style="list-style-type: none">  Notes: <ul style="list-style-type: none"> ▪ For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. ▪ 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 R81.20 ClusterXL Administration Guide.

Step	Instructions
	<p>e. In the Topology section:</p> <ul style="list-style-type: none"> ▪ Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> • Override > Network defined by routes (this is the default). • Override > Specific > select the applicable Network object or Network Group object. ▪ To increase the security, enable the Anti-Spoofing. <p> Important:</p> <ul style="list-style-type: none"> ▪ Make sure the Bridge interface and Bridge subordinate interfaces are not in the Topology. ▪ You cannot define the Topology of the Bridge interface. It is External by default.
15	Click OK .
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 Gateways & Servers .
3	<p>Create a new Cluster object in one of these ways:</p> <ul style="list-style-type: none"> ▪ From the top toolbar, click New (*) > Cluster > Cluster. ▪ In the top left corner, click Objects menu > More object types > Network Object > Gateways and Servers > Cluster > New Cluster. ▪ In the top right corner, click Objects Pane > New > More > Network Object > Gateways and Servers > Cluster > Cluster.
4	<p>In the Check Point Security Gateway Creation window, click Classic Mode.</p> <p>The Gateway Cluster Properties window opens.</p>

Step	Instructions
5	<p>On the General Properties page > Machine section:</p> <ol style="list-style-type: none"> In the Name field, make sure you see the configured applicable name for this ClusterXL object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
6	<p>On the General Properties page > Platform section, select the correct options:</p> <ol style="list-style-type: none"> In the Hardware field: If you install the Cluster Members on Check Point Appliances, select the correct series of appliances. If you install the Cluster Members on Open Servers, select Open server. In the Version field, select R81.20. In the OS field, select Gaia.
7	<p>On the General Properties page:</p> <ol style="list-style-type: none"> On the Network Security tab, make sure the ClusterXL Software Blade is selected. Enable the additional applicable Software Blades on the Network Security tab and on the Threat Prevention tab. <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>

Step	Instructions
8	<p>On the Cluster Members page:</p> <ol style="list-style-type: none">Click Add > New Cluster Member. The Cluster Member Properties window opens.In the Name field, enter the applicable name for this Cluster Member object.Configure the main physical IP address(es) for this Cluster Member object. In the IPv4 Address and IPv6 Address fields, configure the same IPv4 and IPv6 addresses that you configured on the Management Connection page of the Cluster Member's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.  Note - 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.Click Communication.In the One-time password and Confirm one-time password fields, enter the same Activation Key you entered during the Cluster Member's First Time Configuration Wizard.Click Initialize.Click Close.Click OK.Repeat Steps a-h to add the next Cluster Member.

Step	Instructions
	<p>If the Trust State field does not show Trust established, follow these steps:</p> <ol style="list-style-type: none"> 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: <div data-bbox="547 524 1460 589" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> Enter the number of this option: <div data-bbox="547 636 1460 701" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> Follow the instructions on the screen to change the Activation Key. In SmartConsole, click Reset. Enter the same Activation Key you entered in the <code>cpconfig</code> menu. In SmartConsole, click Initialize.
9	<p>On the ClusterXL and VRRP page:</p> <ol style="list-style-type: none"> In the Select the cluster mode and configuration section, select the applicable mode: <ul style="list-style-type: none"> ▪ High Availability and ClusterXL ▪ Load Sharing and Multicast or Unicast ▪ Active-Active In the Tracking section, select the applicable option. In the Advanced Settings section:

Step	Instructions
	<ul style="list-style-type: none"> ■ If you selected the High Availability mode, then: <ol style="list-style-type: none"> i. Optional: Select Use State Synchronization. This configures the Cluster Members to synchronize the information about the connections they inspect. <ul style="list-style-type: none"> ★ Best Practice - Enable this setting to prevent connection drops after a cluster failover. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> i Notes: <ul style="list-style-type: none"> • 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 R81.20 ClusterXL Administration Guide. • The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. • The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.

Step	Instructions
	<p>iv. Select the Cluster Member recovery method - which Cluster Member to select as Active during a fallback (return to normal operation after a cluster failover):</p> <ul style="list-style-type: none">• Maintain current active Cluster Member<ol style="list-style-type: none">i. The Cluster Member that is currently in the Active state, remains in this state.ii. Other Cluster Members that return to normal operation, remain in the Standby state.• Switch to higher priority Cluster Member<ol style="list-style-type: none">i. The Cluster Member that has the highest priority (appears at the top of the list on the Cluster Members page of the cluster object) becomes the new Active.ii. The state of the previously Active Cluster Member changes to Standby.iii. Other Cluster Members that return to normal operation remain in the Standby state.


Step	Instructions
	<ul style="list-style-type: none"> ■ If you selected the Load Sharing > Multicast mode, then: <ol style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> 📘 Notes: <ul style="list-style-type: none"> • 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 R81.20 ClusterXL Administration Guide. • The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. • The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Select the connection sharing method between the Cluster Members:

Step	Instructions
	<ul style="list-style-type: none"> <p data-bbox="675 237 938 271">• IPs, Ports, SPIs</p> <p data-bbox="707 280 1458 432">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.</p> <p data-bbox="707 441 1406 551">This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</p> <p data-bbox="707 560 1461 672">This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p data-bbox="707 680 1110 714">We recommend this method.</p> <p data-bbox="675 723 852 757">• IPs, Ports</p> <p data-bbox="707 766 1458 918">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.</p> <p data-bbox="707 927 1458 1003">Use this method only if there are problems when distributing IPsec packets between Cluster Members.</p> <p data-bbox="675 1012 756 1046">• IPs</p> <p data-bbox="707 1055 1458 1207">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.</p> <p data-bbox="707 1216 1406 1326">This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</p> <p data-bbox="707 1335 1461 1447">This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p data-bbox="707 1456 1458 1568">Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>


Step	Instructions
	<ul style="list-style-type: none"> ■ If you selected the Load Sharing > Unicast mode, then: <ol style="list-style-type: none"> i. Optional: Select Use Sticky Decision Function. This option is available only for clusters R80.10 and lower. For more information, click the (?) button in the top right corner. ii. Optional: Select Start synchronizing [] seconds after connection initiation 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. Range: 2 - 60 seconds Default: 3 seconds <ul style="list-style-type: none"> 📘 Notes: <ul style="list-style-type: none"> • 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 R81.20 ClusterXL Administration Guide. • The greater this value, the fewer short-lived connections the Cluster Members have to synchronize. • The connections that the Cluster Members did not synchronize, do not survive a cluster failover. ★ Best Practice - Enable and configure this setting to increase the cluster performance. iii. Optional: Select Use Virtual MAC. This configures all Cluster Members to associate the same virtual 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 sk50840.

Step	Instructions
	<p>iv. Select the connection sharing method between the Cluster Members:</p> <ul style="list-style-type: none"> <p>• IPs, Ports, SPIs</p> <p>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.</p> <p>This is the least "sticky" sharing configuration that provides the best sharing distribution between Cluster Members.</p> <p>This method decreases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>We recommend this method.</p> <p>• IPs, Ports</p> <p>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.</p> <p>Use this method only if there are problems when distributing IPsec packets between Cluster Members.</p> <p>• IPs</p> <p>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.</p> <p>This is the most "sticky" sharing configuration that provides the worst sharing distribution between Cluster Members.</p> <p>This method increases the probability that a certain connection passes through the same Cluster Member in both inbound and outbound directions</p> <p>Use this method only if there are problems when distributing packets with different port numbers or distributing IPsec packets between Cluster Members.</p>

Step	Instructions
10	<p>On the Network Management page:</p> <ol style="list-style-type: none"> Select each interface and click Edit. The Network: <Name of Interface> window opens. From the left tree, click the General page. In the General section, in the Network Type field, select the applicable type: <ul style="list-style-type: none"> ■ For <i>cluster traffic interfaces</i>, select Cluster. Make sure the Cluster Virtual IPv4 address and its Net Mask are correct. ■ For <i>cluster synchronization interfaces</i>, select Sync or Cluster+Sync. <ul style="list-style-type: none"> i Notes: <ul style="list-style-type: none"> • We do not recommend the configuration Cluster+Sync. • Check Point cluster supports only these settings: <ul style="list-style-type: none"> ◦ One Sync interface. ◦ One Cluster+Sync interface. ◦ One Sync interface and one Cluster+Sync interface. • For Check Point Appliances or Open Servers: The Synchronization Network is supported only on the lowest VLAN tag of a VLAN interface. ■ For <i>interfaces that do not pass the traffic</i> between the connected networks, select Private. In the Member IPs section, make sure the IPv4 address and its Net Mask are correct on each Cluster Member. <ul style="list-style-type: none"> i Notes: <ul style="list-style-type: none"> ■ For a ClusterXL in High Availability mode that is deployed in a Cloud environment (Geo Cluster): You can configure IP addresses that belong to different networks on <i>cluster synchronization interfaces</i> and on <i>cluster traffic interfaces</i>. ■ 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 R81.20 ClusterXL Administration Guide.

Step	Instructions
	<p>e. In the Topology section:</p> <ul style="list-style-type: none"> ▪ Make sure the settings are correct in the Leads To and Security Zone fields. Only these options are supported on cluster interfaces (Known Limitation PMTR-70260): <ul style="list-style-type: none"> • Override > Network defined by routes (this is the default). • Override > Specific > select the applicable Network object or Network Group object. ▪ To increase the security, enable the Anti-Spoofing. <p> Important:</p> <ul style="list-style-type: none"> ▪ Make sure the Bridge interface and Bridge subordinate interfaces are not in the Topology. ▪ You cannot define the Topology of the Bridge interface. It is External by default.
11	Click OK .
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 Security Policies .
3	<p>Create a new policy and configure the applicable layers:</p> <ol style="list-style-type: none"> a. At the top, click the + tab (or press CTRL T). b. On the Manage Policies tab, click Manage policies and layers. c. In the Manage policies and layers window, create a new policy and configure the applicable layers. d. Click Close. e. On the Manage Policies tab, click the new policy you created.
4	<p>Create the applicable rules in the Access Control and Threat Prevention policies.</p> <p> Important - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "Deploying a Security Gateway or a ClusterXL in Bridge Mode" on page 591.</p>

Step	Instructions
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	<p>Examine the cluster state in one of these ways:</p> <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre>show cluster state</pre> ▪ In the Expert mode, run: <pre>cphaprob state</pre> <p>Example output:</p> <pre>Member1> show cluster state Cluster Mode: High Availability (Active Up, Bridge Mode) 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	<p>Examine the cluster interfaces in one of these ways:</p> <ul style="list-style-type: none"> ▪ In Gaia Clish, run: <pre>show cluster members interfaces all</pre> ▪ In the Expert mode, run: <pre>cphaprob -a if</pre>

Step	Instructions
4	<p>Make sure the value of the kernel parameter fwha_monitor_if_link_state is 1 (this is the default). This kernel parameter enables the "Monitoring of the Interface Link State" (MILS) feature.</p> <p>a. Examine the current loaded value:</p> <pre data-bbox="497 443 1460 506">fw ctl get int fwha_monitor_if_link_state</pre> <p>If the current value is not 1, run this command and examine the value:</p> <pre data-bbox="497 595 1460 658">fw ctl set int fwha_monitor_if_link_state 1</pre> <p>b. Examine if this the kernel parameter is configured permanently:</p> <pre data-bbox="497 707 1460 808">grep fwha_monitor_if_link_state \$FWDIR/boot/modules/fwkern.conf</pre> <p>If this the kernel parameter appears in the configuration file, remove its entire line:</p> <pre data-bbox="497 898 1460 960">vi \$FWDIR/boot/modules/fwkern.conf</pre>

Accept, or Drop Ethernet Frames with Specific Protocols

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

By default, a Security Gateway, a Cluster, or a Scalable Platform Security Group 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, a Cluster, or a Scalable Platform Security Group 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, or Scalable Platform Security Group.
2	Log in to the Expert mode.
3	Backup the current <code>/etc/rc.d/init.d/network</code> file: <ul style="list-style-type: none"> ▪ On the Security Gateway / each Cluster Member: <pre>cp -v /etc/rc.d/init.d/network{, _BKP}</pre> ▪ On the Scalable Platform Security Group: <pre>g_cp -v /etc/rc.d/init.d/network{, _BKP}</pre>
4	Edit the current <code>/etc/rc.d/init.d/network</code> file: <pre>vi /etc/rc.d/init.d/network</pre>
5	After the line: <pre>./etc/init.d/functions</pre> Add this line: <pre>/sbin/sysctl -w net.bridge.bpdu_forwarding=0</pre>
6	Save the changes in the file and exit the Vi editor.

Step	Instructions
7	<p>On the Scalable Platform Security Group: Copy the modified file to other Security Group Members:</p> <pre data-bbox="316 309 1461 371">asg_cp2blades -b all /etc/rc.d/init.d/network</pre>
8	<p>Reboot.</p> <ul style="list-style-type: none"><li data-bbox="357 474 1461 577">▪ On the Security Gateway / each Cluster Member:<pre data-bbox="395 515 1461 577">reboot</pre><li data-bbox="357 586 1461 689">▪ On the Scalable Platform Security Group:<pre data-bbox="395 627 1461 689">g_reboot -a</pre>
9	<p>Make sure the new configuration is loaded:</p> <ul style="list-style-type: none"><li data-bbox="357 792 1461 896">▪ On the Security Gateway / each Cluster Member:<pre data-bbox="395 833 1461 896">sysctl net.bridge.bpdu_forwarding</pre><li data-bbox="357 904 1461 1008">▪ On the Scalable Platform Security Group:<pre data-bbox="395 945 1461 1008">g_all sysctl net.bridge.bpdu_forwarding</pre> <p>The output must show:</p> <pre data-bbox="316 1079 1461 1142">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.

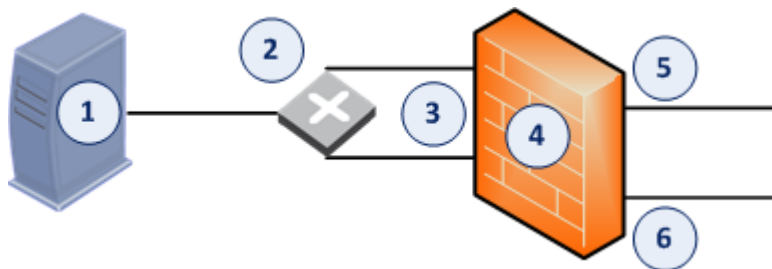
If you configure a Bridge interface with an IP address on a Security Gateway (not on Cluster Members), the Bridge interface functions as a regular Layer 3 interface.

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 subordinate interface of the Bridge interface.
3. The Security Gateway forwards the inspected management packet to the router through the second subordinate interface of the Bridge interface.
4. The router sends the packet to the first subordinate interface 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 <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <p>a. Back up the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre data-bbox="395 949 1428 1014">cp -v \$FWDIR/boot/modules/fwkernel.conf{, _BKP}</pre> <p>If this file does not exist, create it:</p> <pre data-bbox="395 1061 1428 1126">touch \$FWDIR/boot/modules/fwkernel.conf</pre> <p>b. Edit the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre data-bbox="395 1173 1428 1238">vi \$FWDIR/boot/modules/fwkernel.conf</pre> <p>c. Add this line in the file:</p> <pre data-bbox="395 1285 1428 1350">fwx_bridge_reroute_enabled=1</pre> <p> Important - This configuration file does not support spaces or comments.</p> <p>d. Save the changes in the file.</p> <p>e. Exit the Vi editor.</p>
4	<p>Set the value of the required kernel parameter on-the-fly:</p> <pre data-bbox="316 1608 1428 1664">fw ctl set int fwx_bridge_reroute_enabled 1</pre>
5	<p>Make sure the Security Gateway loaded the new configuration:</p> <pre data-bbox="316 1749 1428 1805">fw ctl get int fwx_bridge_reroute_enabled</pre> <p>The output must return</p> <pre data-bbox="316 1861 1428 1917">fwx_bridge_reroute_enabled = 1</pre>

Step	Instructions
6	Reboot the Security Gateway when possible.
7	<p data-bbox="312 300 1430 333">After the reboot, make sure the Security Gateway loaded the new configuration:</p> <pre data-bbox="312 344 1430 400">fw ctl get int fwx_bridge_reroute_enabled</pre> <p data-bbox="312 412 1430 445">The output must return</p> <pre data-bbox="312 456 1430 512">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 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>! Important - In a Cluster, you must configure all the Cluster Members in the same way.</p> <ol style="list-style-type: none"> Connect to the command line on the Security Gateway. Log in to the Expert mode. Back up the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file: <pre data-bbox="384 689 1458 752">cp -v \$FWDIR/boot/modules/fwkernel.conf{,_BKP}</pre> Edit the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file: <pre data-bbox="384 801 1458 864">vi \$FWDIR/boot/modules/fwkernel.conf</pre> Add this line (spaces or comments are not allowed): <pre data-bbox="384 913 1458 976">fwaccept_unknown_protocol=0</pre> Save the changes in the file and exit the editor. Reboot the Security Gateway. <p>If the reboot is not possible at this time, then:</p> <ul style="list-style-type: none"> ▪ Run this command to make the required change: <pre data-bbox="464 1151 1458 1214">fw ctl set int fwaccept_unknown_protocol 0</pre> ▪ Run this command to make sure the required change was accepted: <pre data-bbox="464 1263 1458 1326">fw ctl get int fwaccept_unknown_protocol</pre>

Step	Instructions
2	<p>On the Management Server, edit the applicable <code>user.def</code> file.</p> <p> Note - For the list of <code>user.def</code> files, see sk98239.</p> <ol style="list-style-type: none"> Back up the current applicable <code>user.def</code> file. Edit the current applicable <code>user.def</code> file. Add these directives: <ul style="list-style-type: none"> <code>allowed_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to accept <code>dropped_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to drop <p>Example</p> <pre data-bbox="416 734 1460 1272"> \$ifndef __user_def__ \$define __user_def__ \\ \\ User defined INSPECT code \\ allowed_ethernet_protocols={ <0x0800,0x86DD,0x0806>} ; dropped_ethernet_protocols={ <0x8137,0x8847,0x9100> }; endif /* __user_def__ */ </pre> <p>For the list of EtherType numbers, see http://standards-oui.ieee.org/ethertype/eth.csv.</p> <ol style="list-style-type: none"> Save the changes in the file and exit the editor.
3	<p>In SmartConsole, install the Access Control Policy on this Security Gateway object.</p>

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 subordinate port goes down, the other bridged subordinate 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.  Note - 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.
3	<p>Back up the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre>cp -v \$FWDIR/boot/modules/fwkernel.conf{,_BKP}</pre> <p>If this file does not exist, create it:</p> <pre>touch \$FWDIR/boot/modules/fwkernel.conf</pre>
4	<p>Edit the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre>vi \$FWDIR/boot/modules/fwkernel.conf</pre>
5	<p>Add this line:</p> <pre>fw_link_state_propagation_enabled=1</pre>
6	Save the changes in the file and exit the Vi editor.
7	Reboot the Security Gateway or <i>each</i> Cluster Member.
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	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 <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre data-bbox="352 277 1458 338">cp -v \$FWDIR/boot/modules/fwkernel.conf{, _BKP}</pre> <p>If this file does not exist, create it:</p> <pre data-bbox="352 389 1458 450">touch \$FWDIR/boot/modules/fwkernel.conf</pre>
4	<p>Edit the current <code>\$FWDIR/boot/modules/fwkernel.conf</code> file:</p> <pre data-bbox="352 533 1458 593">vi \$FWDIR/boot/modules/fwkernel.conf</pre>
5	<p>Add these lines (you can configure up to four LSP pairs):</p> <pre data-bbox="352 680 1458 949">fw_link_state_propagation_enabled=1 fw_manual_link_state_propagation_enabled=1 fw_lsp_pair1="<interface_name_1,interface_name_2>" fw_lsp_pair2="<interface_name_3,interface_name_4>" fw_lsp_pair3="<interface_name_5,interface_name_6>" fw_lsp_pair4="<interface_name_7,interface_name_8>"</pre> <p>Example:</p> <pre data-bbox="352 1001 1458 1099">fw_lsp_pair1="eth1,eth2" fw_lsp_pair2="eth3,eth4"</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>

Step	Instructions
8	<p>Make sure the Security Gateway or Cluster Members loaded the new configuration:</p> <p>a. Output of this command</p> <pre data-bbox="432 383 1458 443">fw ctl get int fw_link_state_propagation_enabled</pre> <p>must return</p> <pre data-bbox="432 495 1458 555">fw_link_state_propagation_enabled = 1</pre> <p>b. Output of this command</p> <pre data-bbox="432 607 1458 707">fw ctl get int fw_manual_link_state_propagation_enabled</pre> <p>must return</p> <pre data-bbox="432 759 1458 819">fw_manual_link_state_propagation_enabled = 1</pre> <p>c. Output of this command</p> <pre data-bbox="432 871 1458 931">fw ctl get str fw_lsp_pair1</pre> <p>must return the names of the interfaces configured in this pair</p> <pre data-bbox="432 983 1458 1043"><interface_name_1,interface_name_2></pre> <p>d. Output of this command</p> <pre data-bbox="432 1095 1458 1155">fw ctl get str fw_lsp_pair2</pre> <p>must return the names of the interfaces configured in this pair</p> <pre data-bbox="432 1207 1458 1267"><interface_name_3,interface_name_4></pre> <p>e. Output of this command</p> <pre data-bbox="432 1319 1458 1379">fw ctl get str fw_lsp_pair3</pre> <p>must return the names of the interfaces configured in this pair</p> <pre data-bbox="432 1431 1458 1491"><interface_name_5,interface_name_6></pre> <p>f. Output of this command</p> <pre data-bbox="432 1543 1458 1603">fw ctl get str fw_lsp_pair4</pre> <p>must return the names of the interfaces configured in this pair</p> <pre data-bbox="432 1655 1458 1715"><interface_name_7,interface_name_8></pre>

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.

i 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 [R81.20 CLI Reference Guide](#):

Command	Description
<code>\$CPDIR/bin/cpstat -f policy fw</code>	Shows the currently installed policy
<code>\$FWDIR/bin/control_bootsec {-r -R}</code>	Disables the boot security
<code>\$FWDIR/bin/control_bootsec [-g -G]</code>	Enables the boot security
<code>\$FWDIR/bin/comp_init_policy [-u -U]</code>	Deletes the local state policy
<code>\$FWDIR/bin/comp_init_policy [-g -G]</code>	Creates the local state Initial Policy
<code>\$FWDIR/bin/fw unloadlocal</code>	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"> ▪ Drops all incoming packets that have the same source IP addresses as the IP addresses assigned to the Security Gateway interfaces ▪ Allows all outbound packets from the Security Gateway
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> Best Practice - If the boot process requires that the Security Gateway communicate with other hosts, do not 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"> ▪ Allows all DHCP Requests ▪ Allows all DHCP Replies ▪ Uses Boot Filter: <ul style="list-style-type: none"> a. Drops all incoming packets that have the same source IP addresses as the IP addresses assigned to the Security Gateway interfaces b. Allows all outbound packets from the Security Gateway

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	<p>Back up the current Default Filter Policy file:</p> <pre data-bbox="347 1816 1449 1877">cp -v \$FWDIR/conf/defaultfilter.pf{, _BKP}</pre>

Step	Instructions
5	<p>Create a new Default Filter Policy file.</p> <ul style="list-style-type: none"> To create a new Boot Filter, run: <pre data-bbox="432 342 1449 443">cp -v \$FWDIR/lib/defaultfilter.boot \$FWDIR/conf/defaultfilter.pf</pre> To create a new Drop Filter, run: <pre data-bbox="432 495 1449 595">cp -v \$FWDIR/lib/defaultfilter.drop \$FWDIR/conf/defaultfilter.pf</pre> To create a new DAG Filter, run: <pre data-bbox="432 647 1449 748">cp -v \$FWDIR/lib/defaultfilter.dag \$FWDIR/conf/defaultfilter.pf</pre>
6	<p>Compile the new Default Filter file:</p> <pre data-bbox="352 831 1449 891">fw defaultgen</pre> <ul style="list-style-type: none"> The new compiled Default Filter file for IPv4 traffic is: <pre data-bbox="432 965 1449 1025">\$FWDIR/state/default.bin</pre> The new compiled Default Filter file for IPv6 traffic is: <pre data-bbox="432 1077 1449 1137">\$FWDIR/state/default.bin6</pre>
7	<p>Get the path of the Default Filter Policy file:</p> <pre data-bbox="352 1223 1449 1283">\$FWDIR/boot/fwboot bootconf get_def</pre> <p>Example:</p> <pre data-bbox="352 1335 1449 1435">[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"> For IPv4 traffic, run: <pre data-bbox="432 1581 1449 1682">cp -v \$FWDIR/state/default.bin /etc/fw.boot/default.bin</pre> For IPv6 traffic, run: <pre data-bbox="432 1733 1449 1834">cp -v \$FWDIR/state/default.bin6 /etc/fw.boot/default.bin6</pre>

Step	Instructions
9	<p>Make sure to connect to the Security Gateway over a serial console.</p> <p>i Important - 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.

i 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.
3	Log in to the Expert mode.
4	<p>Back up the current Default Filter Policy file:</p> <pre>cp -v \$FWDIR/conf/defaultfilter.pf{, _BKP}</pre>
5	<p>Create a new Default Filter Policy file.</p> <ul style="list-style-type: none"> ▪ To use the Boot Filter as a template, run: <pre>cp -v \$FWDIR/lib/defaultfilter.boot \$FWDIR/conf/defaultfilter.pf</pre> ▪ To use the Drop Filter as a template, run: <pre>cp -v \$FWDIR/lib/defaultfilter.drop \$FWDIR/conf/defaultfilter.pf</pre> ▪ To use the DAG Filter as a template, run: <pre>cp -v \$FWDIR/lib/defaultfilter.dag \$FWDIR/conf/defaultfilter.pf</pre>

Step	Instructions
6	<p>Edit the new Default Filter Policy file to include the applicable INSPECT code.</p> <p> Important - Your customized Default Filter must not use these functions:</p> <ul style="list-style-type: none"> ▪ Logging ▪ Authentication ▪ Encryption ▪ Content Security
7	<p>Compile the new Default Filter file:</p> <pre data-bbox="352 589 1458 651">fw defaultgen</pre> <ul style="list-style-type: none"> ▪ The new compiled Default Filter file for IPv4 traffic is: <pre data-bbox="432 723 1458 786">\$FWDIR/state/default.bin</pre> ▪ The new compiled Default Filter file for IPv6 traffic is: <pre data-bbox="432 835 1458 898">\$FWDIR/state/default.bin6</pre>
8	<p>Get the path of the Default Filter Policy file:</p> <pre data-bbox="352 978 1458 1041">\$FWDIR/boot/fwboot bootconf get_def</pre> <p>Example:</p> <pre data-bbox="352 1090 1458 1229">[Expert@MyGW:0]# \$FWDIR/boot/fwboot bootconf get_def /etc/fw.boot/default.bin [Expert@MyGW:0]#</pre>
9	<p>Copy new compiled Default Filter file to the path of the Default Filter Policy file.</p> <ul style="list-style-type: none"> ▪ For IPv4 traffic, run: <pre data-bbox="432 1375 1458 1480">cp -v \$FWDIR/state/default.bin /etc/fw.boot/default.bin</pre> ▪ For IPv6 traffic, run: <pre data-bbox="432 1529 1458 1635">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> Important - 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	<p>Reboot the Security Gateway.</p>

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"> ▪ Shuts down Check Point processes ▪ Loads the Default Filter policy (<code>defaultfilter</code>)
<pre>cpstop - fwflag - proc</pre>	<ul style="list-style-type: none"> ▪ Shuts down Check Point processes ▪ Keeps the currently loaded kernel policy ▪ 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" <p> Note - 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 Start in maintenance mode .
5	Enter the Expert mode password.
6	<p>Set the Default Filter to not load again:</p> <ol style="list-style-type: none"> Go to the <code>\$FWDIR</code> directory: <pre>cd /opt/CPsuite-<VERSION>/fw1/</pre> Set the Default Filter to not load again: <pre>./fwboot bootconf set_def</pre>
7	<p>In the <code>\$FWDIR/boot/boot.conf</code> file, examine the value of the "DEFAULT_FILTER_PATH":</p> <ol style="list-style-type: none"> Go to the <code>\$FWDIR</code> directory: <pre>cd /opt/CPsuite-<VERSION>/fw1/</pre> examine the value of the "DEFAULT_FILTER_PATH": <pre>grep DEFAULT_FILTER_PATH boot/boot.conf</pre>
8	Reboot the Security Gateway.

Working with Licenses

You can manage licenses on your Security Gateways in these ways:

- In SmartConsole you can activate, add, or delete your licenses. See "[Viewing Licenses in SmartConsole](#)" on page 681 and "[Managing Licenses in SmartConsole](#)" on page 688.
- In Gaia Portal, you can activate, add, or delete your licenses. See "[Managing Licenses in the Gaia Portal](#)" on page 692.
- In Gaia Clish or the Expert mode, you can add or delete your licenses with the "cplic" command.

See the [R81.20 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 696.

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

To view license information

Step	Instructions
1	From the left navigation panel, click Gateways & Servers .
2	From the Columns drop-down list, select Licenses .

You can see these columns:

Column	Description
License Status	<p>The general state of the Software Blade licenses:</p> <ul style="list-style-type: none"> ▪ OK - All the blade licenses are valid. ▪ Not Activated - 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. ▪ Error with <number> blade(s) - The specified number of blade licenses are not installed or not valid. ▪ Warning with <number> blade(s) - The specified number of blade licenses have warnings. ▪ N/A - No available information.
CK	Unique Certificate Key of the license instance.
SKU	Catalog ID from the Check Point User Center.
Account ID	User's account ID.
Support Level	Check Point level of support.
Support Expiration	Date when the Check Point support contract expires.

To view license information for each Software Blade

Step	Instructions
1	Select a Security Gateway or a Security Management Server.

Step	Instructions
2	<p>In the Summary tab below, click the object's License Status (for example: OK). The Device & License Information window opens. It shows basic object information and License Status, license Expiration Date, and important quota information (in the Additional Info column) for each Software Blade.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ Quota information, quota-dependent license statuses, and blade information messages are only supported for R80 and higher. ▪ The tooltip of the SKU is the product name.

The possible values for the Software Blade **License Status** are:

Status	Description
Active	The Software Blade is active and the license is valid.
Available	The Software Blade is not active, but the license is valid.
No License	The Software Blade is active but the license is not valid.
Expired	The Software Blade is active, but the license expired.
About to Expire	The Software Blade is active, but the license will expire in thirty days (default) or less (7 days or less for an evaluation license).
Quota Exceeded	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.
Quota Warning	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.
N/A	The license information is not available.

Viewing license information for VSX

SmartConsole reports an error when viewing licenses of Virtual System or Virtual Router objects.

To see the VSX license information:

Select the VSX Gateway or VSX Cluster object (and not objects of Virtual Systems or Virtual Routers).

Monitoring Licenses in SmartConsole

To keep track of license issues, you can use these options in SmartConsole:

Option	Instructions
License Status view	To see and export license information for Software Blades on each specific Security Management Server, Security Gateway, or Log Server object.
License Status report	To see filter and export license status information for all configured Security Management Server, Security Gateway, or Log Server objects.
License Inventory report	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 Gateways & Servers .
2	From the top toolbar, click Actions > License Report .

Step	Instructions
3	<p>Wait for the SmartView to load and show this report. By default, this report contains:</p> <ul style="list-style-type: none"> ▪ <i>Inventory</i> page: <ul style="list-style-type: none"> • Blade Names • Devices Names • License Statuses ▪ <i>License by Device</i> page: <ul style="list-style-type: none"> • Devices Names • License statuses • CK • SKU • Account ID • Support Level • Next Expiration Date

Exporting the License Inventory report

Step	Instructions
1	In the top right corner, click the Options button.
2	Select the applicable export option - Export to Excel , or Export to PDF .

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 Logs & Monitor
2	At the top, open a new tab by clicking New Tab , or [+].
3	In the left section, click Views .
4	In the list of reports, double-click License Status .

Step	Instructions
5	<p>Wait for the SmartView to load and show this report. By default, this report contains:</p> <ul style="list-style-type: none"> ▪ Names of the configured objects ▪ License status for each object ▪ CK ▪ SKU ▪ Account ID ▪ Support Level ▪ Next Expiration Date

Filtering the License Status report

Step	Instructions
1	In the top right corner, click the Options button > click View Filter . The Edit View Filter window opens.
2	Select a Field to filter results. For example, Device Name , License Status , Account ID .
3	Select the logical operator - Equals , Not Equals , or Contains .
4	Select or enter a filter value.  Note - Click the X icon to delete a filter.
5	Optional: Click the + icon to configure additional filters.
6	Click OK 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 Options button.
2	Select the applicable export option - Export to Excel , or Export to PDF .

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 Logs & Monitor
2	At the top, open a new tab by clicking New Tab , or [+].
3	In the left section, click Reports .
4	In the list of reports, double-click License Inventory .
5	<p>Wait for the SmartView to load and show this report. By default, this report contains:</p> <ul style="list-style-type: none"> ▪ <i>Inventory</i> page: <ul style="list-style-type: none"> • Blade Names • Devices Names • License Statuses ▪ <i>License by Device</i> page: <ul style="list-style-type: none"> • Devices Names • License statuses • CK • SKU • Account ID • Support Level • Next Expiration Date

Filtering the License Inventory report

Step	Instructions
1	In the top right corner, click the Options button > click Report Filter . The Edit Report Filter window opens.
2	Select a Field to filter results. For example, Blade Name , Device Name , License Overall Status , Account ID .
3	Select the logical operator - Equals , Not Equals , or Contains .

Step	Instructions
4	Select or enter a filter value.  Note - Click the X icon to delete a filter.
5	Optional: Click the + icon to configure additional filters.
6	Click OK 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 Options button.
2	Select the applicable export option - Export to Excel , or Export to PDF .

Managing Licenses in SmartConsole

Starting from R81, you can add or remove licenses manually in SmartConsole.

Adding and removing a license

Step	Instructions
1	In SmartConsole, from the left navigation panel, click Gateways & Servers .
2	In the top pane, select the object of the applicable Management Server or Security Gateway.
3	In the bottom pane, click the Licenses tab.
4	Add or remove a license: <ul style="list-style-type: none">▪ To add a license from a license file:<ol style="list-style-type: none">a. Click Add and select License File.b. Browse for the license file.c. Select the license file.d. Click Open.▪ To add a license from a license string:<ol style="list-style-type: none">a. Click Add and select License String.b. Paste the license string.c. Click OK.▪ To remove a license:<ol style="list-style-type: none">a. Select the license in the leftmost column.b. Click Remove.

Note - To add or remove licenses on the **Licenses** tab, an administrator must have the **Run One Time Script** permission selected in their profile. To assign this permission, in SmartConsole, go to **Manage & Settings > Permissions & Administrators > Permission Profiles**. Open the relevant permission profile, go to **Gateways > Scripts**, and select **Run One-Time Scripts**.

You can see these columns with license information:

Column	Description
IP Address	The IP address, for which this license was generated.
Expiration Date	Date when the Check Point support contract expires.
CK	Unique Certificate Key of the license instance.
SKU	Catalog ID from the Check Point User Center.

Note - SmartConsole R81 and higher does not support viewing a license of Quantum Spark appliances with Gaia Embedded OS (in the "Gateways & Servers" view, select the Security Gateway object > in the bottom pane, click the "Licenses" tab).

Workaround: Use SmartUpdate to view the licenses.

Important - To distribute licenses to CloudGuard IaaS Security Gateways, see the [R81.20 CloudGuard Controller Administration Guide](#).

Viewing Software Blade license information

Step	Instructions
1	From the left navigation panel, click Gateways & Servers .
2	In the top pane, select the object of the applicable Management Server or Security Gateway.
3	In the bottom pane, click the Summary tab.

Step	Instructions
4	<p>Examine the field License Status:</p> <p>The general state of the Software Blade licenses:</p> <ul style="list-style-type: none"> ▪ OK - All the blade licenses are valid. ▪ Not Activated - 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 results in the blade error message. ▪ Error with <number> blade(s) - The specified number of blade licenses are not installed or not valid. ▪ Warning with <number> blade(s) - The specified number of blade licenses have warnings. ▪ N/A - The license information is not available.
5	<p>To see the license information for each Software Blade this license covers, click the license status in the License Status field.</p> <p>(Alternatively, click the Device & License Information link at the bottom and then click the License Status page from the left.)</p> <p>The Device & License Information window opens and shows the License Status page.</p> <p>This page shows:</p> <ul style="list-style-type: none"> ▪ Object name. ▪ General license state. ▪ IP - Object main IP address. ▪ Account ID - User's account ID. ▪ CK - Unique Certificate Key of the license instance. ▪ Support Level - Check Point level of support for this license. ▪ SKU - Catalog ID from the Check PointUser Center. ▪ Support Expiration - Date when the Check Point support contract expires. ▪ Blade Name - Software Blades this license covers. ▪ License Status - See the summary table below. ▪ Expiration Date - Date when the Check Point support contract expires for this Software Blade. ▪ Additional Info - Additional information about this Software Blade configuration.

The possible values for the Software Blade **License Status** are:

Status	Instructions
Active	The Software Blade is active and the license is valid.
Available	The Software Blade is not active, but the license is valid.
No License	The Software Blade is active, but the license is not valid.
Expired	The Software Blade is active, but the license expired.
About to Expire	The Software Blade is active, but the license will expire in 30 days (default) or less (7 days or less for an evaluation license).
Quota Exceeded	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.
Quota Warning	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.
N/A	The license information is not available.


 **Notes:**

- Quota information, quota-dependent license statuses, and blade information messages are only supported for R80 and above.
- The tooltip of the **SKU** field is the product name.

Managing Licenses in the Gaia Portal

 **Note** - If it is necessary to get a license, visit the [Check Point User Center](#).

Adding a license

Step	Instructions
1	In the navigation tree, click Maintenance > Licenses .
2	Click New . The Add License window opens.
3	Enter the license data manually, or click Paste License to enter the data automatically.  Note - The Paste License button only shows in Internet Explorer. For other web browsers, paste the license strings into the empty text field.
4	Click OK .

Deleting a license

Step	Instructions
1	In the navigation tree, click Maintenance > Licenses .
2	Select a license in the table.
3	Click Delete .

Migrating a License to a New IP Address

Check Point licenses are issued for the main IP address of Check Point servers.

If you changed the IP address of your existing Check Point server, 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 Check Point User Center 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 with these commands: <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>cpstop cpstart</pre> </div>
6	<p>In SmartConsole:</p> <ol style="list-style-type: none"> 1. Connect with SmartConsole to the (Primary) Security Management Server. 2. Open the Security Management Server object. 3. In the left tree, click Network Management. 4. Make sure to update the IP Address and topology. 5. Click OK. 6. Publish the SmartConsole session. 7. Install the database: <ol style="list-style-type: none"> a. In the top left corner, click Menu > Install database. b. Select all objects. c. Click Install. d. Click OK.
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 Check Point User Center 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.
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 " Changing the IP Address of a Multi-Domain Server or Multi-Domain Log Server " on page 541.
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 Check Point User Center 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>

Step	Instructions
6	<p>In SmartConsole:</p> <ol style="list-style-type: none">1. Connect with SmartConsole to the applicable Management Server that manages your dedicated Log Server or SmartEvent Server.2. Open the object of your dedicated Log Server or SmartEvent Server.3. In the left tree, click Network Management.4. Make sure to update the IP Address and topology.5. Click OK.6. Publish the SmartConsole session.7. Install the database:<ol style="list-style-type: none">a. In the top left corner, click Menu > Install database.b. Select all objects.c. Click Install.d. Click OK.8. Install the Access Control Policy on all managed Security Gateways that send their logs to your dedicated Log Server or SmartEvent Server.
7	<p>On your DNS Server, map the host name of your dedicated Log Server or SmartEvent Server to the new IP address.</p>

Using Legacy SmartUpdate

When Security Gateways *can* connect to [Check Point User Center](#), they can get and update their licenses and contracts automatically (for more information, see [sk94064](#)).

When Security Gateways **cannot** connect to [Check Point User Center](#):

- Manage your licenses in one of these ways:
 - In SmartConsole. See "[Managing Licenses in SmartConsole](#)" on page 688.
 - With the "cplic" command. See the [R81.20 CLI Reference Guide](#) > Chapter *Security Gateway Commands* > Section *cplic*.
- Manage your contracts in one of these ways:
 - In the legacy SmartUpdate.
 - With the "cplic" command.

The legacy SmartUpdate can also:

- Distribute licenses and software packages for managed Check Point and OPSEC Certified products.
- Provide 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 more information, see "[Installing Software Packages on Gaia](#)" on page 199.

Accessing SmartUpdate

Step	Instructions
1	<p>Open the SmartUpdate in one of these ways:</p> <ul style="list-style-type: none">▪ In SmartConsole, in the top left corner, click Menu > Manage licenses & packages.▪ On the SmartConsole client, run this executable file directly:<ul style="list-style-type: none">• On Windows OS 32-bit:<pre data-bbox="475 591 1460 734">C:\Program Files\CheckPoint\ SmartConsole\<Rxx>\PROGRAM\SmartDistributor.exe</pre>• On Windows OS 64-bit:<pre data-bbox="475 779 1460 922">C:\Program Files (x86)\CheckPoint\ SmartConsole\<Rxx>\PROGRAM\SmartDistributor.exe</pre>
2	<p>In the top left corner, click Menu > View > Menu Bar. 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">▪ A Central license is tied to the IP address of the Management Server.▪ There is one IP address for all licenses.▪ The license remains valid if you change the IP address of the Security Gateway.▪ A license can be moved from one Check Point Security Gateway to another easily.▪ Maximum flexibility.
Local	<p>The Local license is an older method of licensing that is still supported.</p> <ul style="list-style-type: none">▪ A Local license is tied to the IP address of the specific Security Gateway.▪ Cannot be transferred to a Security Gateway with a different IP address.

Licensing Terms for SmartUpdate

Term	Instructions
Add	<p>You can add any license that you receive from the Check Point User Center to the Licenses & Contracts Repository.</p> <ul style="list-style-type: none"> ■ 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. <p>When you add the Local license to the Licenses & Contracts Repository, it also attaches it to the Security Gateway with the IP address, for which the license was issued.</p> <p>See "Adding New Licenses to the Licenses & Contracts Repository" on page 702.</p>
Attach	<p>You can attach a license from the Licenses & Contracts Repository to a managed Security Gateway.</p> <p>See "Attaching a License to a Security Gateway" on page 706.</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 Licenses & Contracts Repository available to other managed Security Gateways.</p> <p>See "Detaching a License from a Security Gateway" on page 707.</p>
Get	<p>You can add information from your managed Security Gateways about the licenses you installed locally.</p> <p>This updates the Licenses & Contracts Repository 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 License & Contract Repository and removes all locally deleted licenses from the Licenses & Contracts Repository.</p> <p>See "Getting Licenses from Security Gateways" on page 708.</p>
Delete	<p>You can delete a license from the Licenses & Contracts Repository.</p> <p>See "Deleting a License from the Licenses & Contracts Repository" on page 705.</p>
Export	<p>You can export a license from the Licenses & Contracts Repository to a file.</p> <p>See "Exporting a License to a File" on page 709.</p>

Term	Instructions
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 "Checking for Expired Licenses" on page 711.</p>
State	<p>The license state depends on whether the license is associated with a managed Security Gateway in the Licenses & Contracts Repository, and whether the license is installed on that Security Gateway.</p> <p>The license state definitions are:</p> <ul style="list-style-type: none"> ▪ Attached - Indicates that the license is associated with a managed Security Gateway in the Licenses & Contracts Repository, and is installed on that Security Gateway. ▪ Unattached - Indicates that the license is not associated with managed Security Gateways in the Licenses & Contracts Repository, and is not installed on managed Security Gateways. ▪ Assigned Indicates that the license that is associated with a managed Security Gateway in the Licenses & Contracts Repository, but has not yet been installed on a Security Gateway.
Upgrade Status	<p>This is a field in the Licenses & Contracts Repository that contains an error message from the User Center when the License Upgrade process fails.</p>
Central License	<p>Attach a Central License to the IP address of your Management Server.</p>
Local License	<p>A Local License 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.</p>
Multi-License File	<p>This is a license file that contains more than one license.</p> <p>The "cplic put" and "cplic add" commands support these files.</p>
Certificate Key	<p>This is a string of 12 alphanumeric characters.</p> <p>This number is unique to each package.</p>
Features	<p>This is a character string that identifies the features of a package.</p>
cplic	<p>A CLI utility to manage local licenses on Check Point computers.</p> <p>For details, see the R81.20 CLI Reference Guide - Chapter <i>Security Management Server Commands</i> - Section <i>cplic</i>.</p>

Viewing the Licenses & Contracts Repository

Step	Instructions
1	Open the SmartUpdate . See " Accessing SmartUpdate " on page 697.
2	Click the Licenses & Contracts 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 [Check Point 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 SmartUpdate . See " Accessing SmartUpdate " on page 697.
2	Click Licenses & Contracts tab.
3	Click Licenses & Contracts menu at the top > Add License > From User Center .
4	Enter your User Center credentials.
5	Click Assets / Info > Product Center .
6	Perform one of the following: <ul style="list-style-type: none"> ▪ Generate a new license, if there are no identical licenses. This adds the license to the Licenses & Contracts Repository. ▪ Change the IP address of an existing license with Move IP. ▪ Change the license from Local to Central.

Adding a license from a file


Step	Instructions
1	In the applicable Check Point User Center account: <ol style="list-style-type: none"> Generate a license. Click the License Information tab. Click the Get Last License. Click the Get License File. Save the CPLicenseFile.lic file.
2	Open the SmartUpdate . See " Accessing SmartUpdate " on page 697.
3	Click the Licenses & Contracts tab.
4	Click the Licenses & Contracts menu at the top > Add License > From File .
5	Locate and select the downloaded CPLicenseFile.lic file.
6	Click Open .
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 Check Point User Center . <p> Notes:</p> <ul style="list-style-type: none"> ▪ User Center sends you an e-mail with the license information. ▪ You can also click the License Information tab to see and copy this information.
2	Open the SmartUpdate . See " Accessing SmartUpdate " on page 697.
3	Click the Licenses & Contracts tab.
4	Click the Licenses & Contracts menu at the top > Add License > Manually .

Step	Instructions
5	<p>In the Add License window you can:</p> <ul style="list-style-type: none">▪ Copy the applicable string from the User Center e-mail and click Paste License.▪ Paste the applicable information you copied from the User Center. <p> Note - If you leave the Name field empty, the license is assigned a name in the format <SKU>@<Time Date>.</p>
6	Click OK .

Deleting a License from the Licenses & Contracts Repository

You can delete an unattached license that is no longer needed:

Step	Instructions
1	Open the SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click the Licenses & Contracts tab.
3	If you do not see the window License And Contract Repository , then click the Licenses & Contracts menu at the top > click View Repository .
4	Right-click anywhere in the Licenses And Contracts Repository window and select View Unattached Licenses .
5	Right-click the Unattached license that you want to delete, and select Delete License / Contract .
6	Click Yes 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 SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click the Licenses & Contracts tab.
3	Click the Licenses & Contracts menu at the top > click Attach .
4	In the Attach Licenses window, select the applicable Security Gateway or Cluster Member.
5	Click Next .
6	Select the applicable license.
7	Click Finish .
8	Check the Operation Status window.
9	Connect to the command line on the applicable Security Gateway or Cluster Member.
10	Run the " <code>cplic print</code> " command to make sure the license is attached.

Detaching a License from a Security Gateway

Step	Instructions
1	Open the SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click the Licenses & Contracts tab.
3	Click the Licenses & Contracts menu at the top > click Detach .
4	In the Detach Licenses window, select the applicable Security Gateway or Cluster Member.
5	Click Next .
6	Select the applicable license.
7	Click Finish .
8	Check the Operation Status window.
9	Connect to the command line on the applicable Security Gateway or Cluster Member.
10	Run the " <code>cplic print</code> " 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 SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click the Licenses & Contracts tab.
3	Click the Licenses & Contracts menu at the top > click Get all Licenses .
4	Check the Operation Status 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 SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click Licenses & Contracts tab.
3	If you do not see the window License And Contract Repository , then click the Licenses & Contracts menu at the top > click View Repository .
4	Right-click anywhere in the Licenses And Contracts Repository window and select View all Licenses & Contracts .
5	Right-click the license that you want to export, and select Export License to File .
6	Select the location, enter the applicable file name and click Save .

 **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 SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click the Licenses & Contracts tab.
3	If you do not see the window License And Contract Repository , then click the Licenses & Contracts menu at the top> View Repository .
4	Right-click anywhere in the Licenses And Contracts Repository window and select View all Licenses & Contracts .
5	Press and hold the CTRL key.
6	Left-click each license that you want to export.
7	Release the CTRL key.
8	Right-click on one of the selected licenses and select Export License to File .

Step	Instructions
9	Select the location, enter the applicable file name and click Save .

 **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 SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click the Licenses & Contracts tab.
3	Click the Licenses & Contracts menu at the top > click Show Expired .
4	In the License/Contract Expiration window, the expired licenses appear in the Expired License and Contracts section.
5	To delete an expired license, select it and click Delete .

Checking for licenses nearing their dates of expiration

Step	Instructions
1	Open the SmartUpdate . See "Accessing SmartUpdate" on page 697 .
2	Click the Licenses & Contracts tab.
3	Click the Licenses & Contracts menu at the top > click Show Expired .
4	In the License/Contract Expiration window, set the applicable number of days in the field Search for licenses/contracts expiring within the next X days .
5	Click Apply 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 Control
 - URL Filtering
 - Threat Prevention (Anti-Bot, Anti-Virus, Anti-Spam, IPS, Threat Emulation)
 - HTTPS Inspection
 - 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 Menu > Global properties > Security Management Access .
2	Select Automatically download Contracts and other important data .
3	Click OK .
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.


This setting activates the Check Point User Center Synchronization Tool. It updates your [Check Point 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 Menu > Global properties > Security Management Access .
2	Select or clear Improve product experience by sending data to Check Point .
3	Click OK .
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.

Glossary

A

Anti-Bot

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

Anti-Spam

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

Anti-Virus

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

Application Control

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

Audit Log

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

B

Bridge Mode

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

C

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

Security Gateway that is part of a cluster.

Compliance

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

Content Awareness

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

CoreXL

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

CoreXL Firewall Instance

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

CoreXL SND

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

CPUSE

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

D

DAIP Gateway

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

Data Loss Prevention

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

Data Type

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

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

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

Dynamic Object

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

E

Endpoint Policy Management

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

Expert Mode

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

G

Gaia

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

Gaia Clish

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

Gaia Portal

Web interface for the Check Point Gaia operating system.

H

Hotfix

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

HTTPS Inspection

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

I

ICA

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

Identity Awareness

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

Identity Logging

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

Internal Network

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

IPS

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

IPsec VPN

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

J

Jumbo Hotfix Accumulator

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

K

Kerberos

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

L

Log Server

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

Logging & Status

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

M

Management Interface

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

Management Server

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

Manual NAT Rules

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

Migration

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

Mobile Access

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

Multi-Domain Log Server

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

Multi-Domain Server

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

N

Network Object

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

Network Policy Management

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

O

Open Server

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

P

Provisioning

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

Q

QoS

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

R

Rule

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

Rule Base

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

S

SecureXL

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

Security Gateway

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

Security Management Server

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

Security Policy

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

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.

SmartConsole

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

SmartDashboard

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

SmartProvisioning

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

SmartUpdate

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

Software Blade

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

Standalone

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

T

Threat Emulation

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

Threat Extraction

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

U

Updatable Object

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

URL Filtering

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

User Directory

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

V

VSX

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

VSX Gateway

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

Z

Zero Phishing

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