Check Point
SOFTWARE TECHNOLOGIES LTD.

27 June 2018

R80.20

Management Feature Release

R80.20.M1

RELEASE NOTES

Restricted

© 2018 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 http://www.checkpoint.com/copyright.html for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html 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 https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Check Point R80.20 Management Feature Release

For more about this release, see the **R80.20 Management Feature Release** home page http://supportcontent.checkpoint.com/solutions?id=sk123473.

Latest Version of this Document

Download the latest version of this document in PDF format http://supportcontent.checkpoint.com/documentation_download?ID=65666.

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R80.20 Management Feature Release Release Notes.

Revision History

Date	Description
27-Jun-18	First release of this document

Contents

Introduction

In This Section:

Management Feature Releases

Check Point further enhances its Security Management with new features, stability fixes and more frequent releases. These enhancements are delivered using a new release path called "Management Feature Release". The first such release is R80.20.M1.

Management Feature Releases are recommended for customers who want to use the latest available Security Management capabilities.

Customers using this release should be prepared to frequently upgrade their management environment when a new such release becomes available.

When the next major release is available (such as R80.20), you can upgrade from the Management Feature Release.

The next major release will include new features and enhancements for the Security Gateway and additional enhancements and features for the Security Management Server.

Before you install this version read this document carefully, as well as the associated Known Limitations found in - sk122486 http://supportcontent.checkpoint.com/solutions?id=sk122486.

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.

Important Links

For more about R80.20 Management Feature Release and to download the software, see the R80.20 Management Feature Release Home Page: sk123473 http://supportcontent.checkpoint.com/solutions?id=sk123473.

For the Known Limitations see sk122486 http://supportcontent.checkpoint.com/solutions?id=sk122486.

For the resolved issues in this release see sk122488 http://supportcontent.checkpoint.com/solutions?id=sk122488.

Visit the Check Point CheckMates Community https://community.checkpoint.com/ to:

- Start discussions
- Get answers from experts
- Join the API community to get code samples and share yours

To learn more about R80.20 Management Feature Release visit http://www.checkpoint.com/architecture/infinity/

What's New

R80.20 Management Feature Release is part of **Check Point Infinity**, a consolidated cyber security architecture that spans networks, cloud, and mobile. It provides the highest level of threat prevention against both known and unknown targeted attacks to keep you protected now and in the future.

Threat Prevention

- Threat Prevention Indicators (IoC) API
  - Management API support for Threat Prevention Indicators (IoC).
  - Add, delete, and view indicators through the management API.
- Threat Prevention Layers
  - Support layer sharing within Threat Prevention policy.
  - Support setting different administrator permissions per Threat Prevention layer.

Gaia OS

- Upgraded Linux kernel (3.10)
- New file system (xfs)
  - More than 2TB support per a single storage device
  - Enlarged systems storage (up to 48TB)
- I/O related performance improvements
- Support of new system tools for debugging, monitoring and configuring the system
  - `iotop` (provides I/O runtime stats)
  - `lsusb` (provides information about all devices connected to USB)
  - `lshw` (provides detailed information about all hardware)
  - `lsscsi` (provides information about storage)
  - `ps` (new version, more counters)
  - `top` (new version, more counters)
  - `iostat` (new version, more counters)
- Compressed snapshots - reduced system snapshot size.

Access Policy

- Rule Base performance improvements, for enhanced Rule Base navigation and scrolling.
- Global VPN Communities (previously supported in R77.30).
- Access Control visibility for NAT46 and NAT64.
- Identify Tags: Access Role objects can manage identities that originated from Cisco ISE Security Groups or Check Point Identity Awareness API.
- Ability to use an Identity Awareness Security Gateway as a proxy to connect to the Active Directory environment, if the Security Management Server has no connectivity to the Active Directory environment and the gateway does.

Logging and Monitoring

- SmartView (web) enhancements:
  - Auto-refresh views
  - Improved log-viewer with cards, profiles, statistics and filters
  - Export logs with custom or all fields
- Keyboard-navigation
- Ability to define an external Syslog server object and configure the Security Gateway to send all its logs to it (previously supported in R77.30)
- Log Exporter - an easy and secure method to export Check Point logs over syslog that utilizes standard protocols and formats.

SmartProvisioning

- Integration with SmartProvisioning (previously supported in R77.30).
- Support for the 1400 series appliances.
- Administrators can now use SmartProvisioning in parallel with SmartConsole.

SmartConsole

- Multiple simultaneous sessions in SmartConsole. One administrator can publish or discard several SmartConsole private sessions, independently of the other sessions.

CloudGuard IaaS Enhancements

- Integration with Google Cloud Platform.
- Integration with Cisco ISE.
- Integration with Nuage Networks.
- Automatic license management with the CloudGuard IaaS Central Licensing utility.
- Monitoring capabilities integrated into SmartView.
- CloudGuard IaaS support for 41000, 44000, 61000, and 64000 Scalable Platforms.

Endpoint Security Server

Managing features that are included in R77.30.03:

- Management of new Software Blades:
  - SandBlast Agent Anti-Bot.
  - SandBlast Agent Threat Emulation and Anti-Exploit.
  - SandBlast Agent Forensics and Anti-Ransomware.
  - Capsule Docs.
- New features in existing blades:
  - Full Disk Encryption.
    - Offline Mode.
    - Self Help Portal.
    - XTS-AES Encryption.
    - New options for the Trusted Platform Module (TPM).
    - New options for managing Pre-Boot Users.
  - Media Encryption & Port Protection.
    - New options to configure encrypted container.
    - Optical Media Scan.
  - Anti-Malware:
    - Web Protection.
    - Advanced Disinfection.

Additional Enhancements

- Improvements in policy installation performance on R80.10 and higher Security Gateways with IPS.
- Compliance:
  - User can create custom best practices based on scripts.
  - Support for 35 regulations including General Data Protection Regulation (GDPR).

Licensing

For all licenses issues contact Account Services
mailto:accountservices@checkpoint.com?subject=Licensing Issues.

Supported Upgrade Paths

CPUSE is the installation and upgrade method supported for this release. To learn more about CPUSE, see sk92449 http://supportcontent.checkpoint.com/solutions?id=sk92449.

R80.20 Management Feature Release supports Linux 3.10 kernel. When you perform a Clean Install, or Advanced Upgrade to R80.20 Management Feature Release, it uses the *xfs* file system. After an in-place upgrade (using CPUSE), the file system remains *ext3* except for Smart-1 525, 5050, 5150 appliances, which use the *xfs* file system.

Upgrade with the Supported Methods for your current installation.

From R75.4x, R75.40VS, R76, R77.x, R77.30.01, R77.30.02, R77.30.03, R80, R80.10 to R80.20 Management Feature Release:

Item	Description
Security Management Server Multi-Domain Server CloudGuard IaaS	• CPUSE Upgrade • CPUSE Clean Install • Advanced Upgrade

Notes:

- **To upgrade from R77.20 or R77.30 with the Add-on:** It is not necessary to uninstall the Add-on. Remove these unsupported features: Modbus support with the Application Control Software Blade, and "SAML" Cloud Connector for web based single sign on.
- **Downgrade**: On Smart-1 525, Smart-1 5050, and Smart-1 5150 appliances (sk120453 http://supportcontent.checkpoint.com/solutions?id=sk120453) that run the Dedicated R80.10 image:

  Before upgrading to R80.20 Management Feature Release, take a Gaia OS Snapshot. If in the future you decide to downgrade the appliance back to the Dedicated R80.10 image, revert to that Gaia OS Snapshot.
- **During the upgrade from R80 only:**
  - User Defined reports are migrated to the SmartConsole reports.
  - Report Scheduling and email server definitions are not migrated and need to be defined again.

Required Disk Space

Required Disk Space for Security Management Server:

Before installation or upgrade, CPUSE verifies that enough free disk space is available. If the amount of available disk space is not sufficient, a message shows what is required.

This table shows the free disk space required for some packages:

R80.20 Installation, or Upgrade Type	Required Disk Space
Clean Install	The minimum required unpartitioned disk space is the highest value of one of these: • Size of the current root partition. • The used space in the current root partition plus 3 GB. • If the used space is more than 90% of the root partition, then 110% of the size of the current root partition.
Major Upgrade	

If you do not have enough free disk space, you can use the Logical Volume Manager (LVM) to increase the disk space of logical volumes on Gaia. This space is taken from the unallocated disk space, which is usually used for snapshots and upgrades. For more details see sk95566 http://supportcontent.checkpoint.com/solutions?id=sk95566.

Required Disk Space for Multi-Domain Security Management Server:

Before you run a clean install of R80.20 Management Feature Release Multi-Domain Servers, make sure that at least **10 GB** of free disk space in the root partition is available. For an environment with many Domain Management Servers, more than 10 GB of free disk space is often required.

Check Point Appliances

Management Servers boot by default with 64-bit Gaia kernel after a clean install or upgrade to R80.20.

Note - If you revert from the R80.20 Management Feature Release upgrade, the appliance will still boot with 64-bit Gaia kernel, even if it was originally 32-bit.

Management Servers

Check Point Product	Smart-1 25b, 205, 210, 225, 405, 410, 525	Smart-1 50, 150, 3050, 3150, 5050, 5150
Security Management Server	✓	✓
Log Server	✓	✓
SmartEvent Server	✓	✓
Multi-Domain Security Management Server		✓
Multi-Domain Log Server		✓

* Smart-1 25B, 205, and 210 appliances with default memory can run Security Management *OR* Log Server *OR* SmartEvent.

** We recommend that you upgrade the memory of Smart-1 205 to 16GB as part of the upgrade to R80.20 Management Feature Release.

*** Smart-1 210 with memory extension to 16GB can run Security Management AND/OR Log Server AND/OR SmartEvent.

Hardware Health Monitoring

R80.20 Management Feature Release supports these Hardware Health Monitoring features for Gaia Check Point appliances:

- **RAID Health:** Use SNMP to monitor the health of the disks in the RAID array, and be notified of volume and disk states.
- **Hardware Sensors:** Use the Gaia Portal or SNMP to monitor fan speed, motherboard voltages, power supply health, and temperatures. Some open servers are supported with an IPMI interface card that requires an IPMI card.

Check Point Appliances	Smart-1
SNMP Hardware sensor monitoring (polling and traps)	✓
Gaia Portal hardware sensor monitoring	✓
RAID monitoring with SNMP	✓

Open Server Hardware Requirements

In This Section:

R80.20 Management Feature Release is designed to utilize available hardware resources efficiently to maximize performance and scalability. We recommend that you leverage this advantage and use the most powerful hardware available to get the best performance.

Component	Security Management Server	Multi-Domain Server
Processor	Intel Pentium IV, 2.6 GHz or equivalent	Dual Socket 2x Xeon E5-2609v2 4 cores, 2.5 GHz or equivalent
Total CPU Cores	2	8
Memory	6 GB RAM	32 GB RAM
Free Disk Space	500 GB (Installation includes OS)	1 TB (Installation includes OS)

Maximum Supported Physical Memory

Check Point Product	Physical RAM Limit
Security Management Server, or Multi-Domain Security Management Server	512 GB

Supported Platforms

Check Point Product	Red Hat Enterprise Linux	VMware ESXi	Microsoft Hyper-V**
Security Management Server	5.5, 5.9, 6.8, 7.3	5.x, 6.x	Windows 2012 R2, 2016 (64-bit only)*
Multi-Domain Security Management Server	5.5, 5.9, 6.8, 7.3	5.x, 6.x	Windows 2012 R2, 2016 (64-bit only)*

* For the most up-to-date information about Microsoft Hyper-V, see the *Virtual Machines* section of the Hardware Compatibility List https://www.checkpoint.com/support-services/hcl/.

Build Numbers

Software Blade / Product	Build Number	Verifying Build Number
Gaia	OS build 14	`show version all`
Security Management Server	This is Check Point Security Management Server R80.20.M1 - Build 003	`fwm ver`
Multi-Domain Server	This is Check Point Multi-Domain Security Management R80.20.M1 - Build 003	`fwm mds ver`
SmartConsole	992000006	Menu > About Check Point SmartConsole

Supported Backward Compatibility Gateways

R80.20 Management Feature Release Management Servers can manage Security Gateways of these versions:

Gateway Type	Release Version
Security Gateway	R75.20, R75.30, R75.40, R75.45, R75.46, R75.47, R76, R77, R77.10, R77.20, R77.30, R80.10
VSX	R76, R77, R77.10, R77.20, R77.30, R80.10

R80.20 Management Feature Release Management Servers can manage appliance Security Gateways that run these versions:

Appliance	Release Version
Security Gateway 80	R75.20.x
UTM-1 Edge N	8.1 and higher
1100 Appliances	R75.20.x, R77.20.x
1200R Appliances	R77.20.x
1400 Appliances	R77.20.x
60000/40000 Scalable Platforms	R76SP, R76SP.10, R76SP.20, R76SP.30, R76SP.40 for 61000/41000 R76SP.50 for 61000/41000 and 64000/44000

Logging Requirements

In This Section:

Storing Logs

Logs can be stored on:

- A Security Management Server that collects logs from the Security Gateways. This is the default.
- A Log Server on a dedicated machine. This is recommended for organizations that generate many logs.

A dedicated Log Server has greater capacity and performance than a Security Management Server with an activated logging service. On dedicated Log Servers, the Log Server must be the same version as the Management Server.

SmartEvent Requirements

You can install a SmartEvent Server on a Security Management Server or on a different, dedicated server. SmartEvent R80.20 Management Feature Release can connect to a different version of Log Server - R77.xx or lower.

SmartEvent and a Correlation Unit are usually installed on the same server. You can also install them on separate servers, for example, to balance the load in large logging environments. The Correlation unit must be the same version as SmartEvent.

To deploy SmartEvent and to generate reports, a valid license or contract is required.

When upgrading a Log Server, Multi-Domain Security Management or Multi-Domain Log Server and SmartEvent from R80.x to R80.20 Management Feature Release, log indexes are no longer valid. Re-indexing occurs for logs from the last 24 hours only.

Log history is searchable only if you open a specific log file.

SmartConsole Requirements

In This Section:

Hardware Requirements

This table shows the minimum hardware requirements for SmartConsole applications:

Component	Minimal Requirement
CPU	Intel Pentium Processor E2140, or 2 GHz equivalent processor
Memory	4 GB
Available Disk Space	2 GB
Video Adapter	Minimum resolution: 1024 x 768

Software Requirements

SmartConsole is supported on:

- Windows 10 (all editions), Windows 8.1 (Pro), and Windows 7 (SP1, Ultimate, Professional, and Enterprise).
- Windows Server 2016, 2012, 2008 (SP2), and 2008 R2 (SP1).

Gaia Portal Requirements

The Gaia Portal supports these web browsers:

Browser	Supported Versions
Google Chrome	14 and higher
Microsoft Internet Explorer	8 and higher (If you use Internet Explorer 8, file uploads through the Gaia Portal are limited to 2 GB.)
Microsoft Edge	Any
Mozilla Firefox	6 and higher
Apple Safari	5 and higher

Endpoint Security Requirements

- Endpoint Security Management Servers are supported on Management-only appliances or open servers. Standalone (Security Gateway + Management Server) and Multi-Domain Security Management deployments are not supported.
- Endpoint Security Management Servers are not supported on Red Hat Enterprise Linux releases.
- R80.20 Management Feature Release Endpoint Security Management Server can manage:
  - E80.64 and higher versions of Endpoint Security Clients for Windows.
  - E80.64 Endpoint Security Client for Mac.

Endpoint Security Clients acquire their Anti-Malware signature updates directly from an external Check Point signature server or other external Anti-Malware signature resources, as allowed by your organization's Endpoint Anti-Malware policy. If your organization wants to continue using signature updates from the Endpoint Management Server see sk127074 http://supportcontent.checkpoint.com/solutions?id=sk127074 for more information.

For more information, see the *R80.20 Endpoint Security Administration Guide* https://sc1.checkpoint.com/documents/R80.20_M1/WebAdminGuides/EN/CP_R80.20_M1_EndpointSecurity_AdminGuide/html_frameset.htm

Self-Help Portal for Endpoint Security Full Disk Encryption

The Self-Help Portal lets users reset their own passwords for Full Disk Encryption

These browsers and devices are supported:

Mobile:

- Google Chrome 41 or higher (Android 4 or higher)
- Android Browser (Android 6 or higher)
- Safari (iOS 6.1.3 or higher)

Desktop;

- Internet Explorer 9-11
- Mozilla Firefox 36.0.1 or higher
- Google Chrome 41 or higher