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.

Check Point R80
For more about this release, see the R80 home page http://supportcontent.checkpoint.com/solutions?id=sk108623.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=46538.
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 Release Notes.

Searching in Multiple PDFs
To search for text in all the R80 PDF documents, download and extract the complete R80 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=46577.
Use Shift-Control-F in Adobe Reader or Foxit reader.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 September 2017</td>
<td>Updated Check Point Appliances (on page 12)</td>
</tr>
<tr>
<td>12 June 2017</td>
<td>Update: We recommend that customers install or upgrade to R80.10. See the R80.10 home page <a href="http://supportcontent.checkpoint.com/solutions?id=sk111841">http://supportcontent.checkpoint.com/solutions?id=sk111841</a>.</td>
</tr>
<tr>
<td>26 December 2016</td>
<td>New R80 image for installation and upgrade and new SmartConsole, include R80 Jumbo Hotfix take 76 <a href="http://supportcontent.checkpoint.com/solutions?id=sk111536">http://supportcontent.checkpoint.com/solutions?id=sk111536</a>. See new build numbers on page 9. Clarified Check Point Appliances (on page 12)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>08 June 2016</td>
<td>Added Check Point Appliances (on page 12)</td>
</tr>
<tr>
<td></td>
<td>Added Open Server Hardware Recommendations (on page 12)</td>
</tr>
<tr>
<td></td>
<td>Improved formatting and document layout</td>
</tr>
<tr>
<td>25 April 2016</td>
<td>Added VMware servers to Supported Check Point Installations (on page 11)</td>
</tr>
<tr>
<td></td>
<td>All Known Limitations are in sk108624</td>
</tr>
<tr>
<td></td>
<td><a href="http://supportcontent.checkpoint.com/solutions?id=sk108624">http://supportcontent.checkpoint.com/solutions?id=sk108624</a></td>
</tr>
<tr>
<td></td>
<td>Improved formatting and document layout</td>
</tr>
<tr>
<td>31 March 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

Thank you for installing Check Point R80. This release is for Check Point Security Management Servers and Multi-Domain Servers only. R80 Servers can manage Check Point Security Gateways of previous versions.

For a list of compatible Security Gateways, see Compatibility with Gateways (on page 11).

Important Notes

Effective May 17, 2017:

We recommend that customers install or upgrade to R80.10. See the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

Effective December 26, 2016:

- The R80 image for installation and upgrade has been replaced. The new R80 image includes the R80 Jumbo Hotfix take 76 http://supportcontent.checkpoint.com/solutions?id=sk111536.
- The R80 SmartConsole has been replaced. The new R80 SmartConsole includes fixes listed in the R80 Jumbo Hotfix Take 76 http://supportcontent.checkpoint.com/solutions?id=sk111536.
- The new R80 SmartConsole also supports earlier R80 GA images (takes 113, 109 and 103).

All new images are available from the R80 Home Page: sk108623 http://supportcontent.checkpoint.com/solutions?id=sk108623

R80 Jumbo Hotfix Accumulator is an accumulative release: Take 76 includes all previous R80 Jumbo Hotfix content.

Important Links

- For more about R80 and to download the software, see the R80 Home Page: sk108623 http://supportcontent.checkpoint.com/solutions?id=sk108623
- For more about R80 Image updates, see sk110980 http://supportcontent.checkpoint.com/solutions?id=sk110980
- When upgrading to R80, use the latest upgrade tools from sk108623 http://supportcontent.checkpoint.com/solutions?id=sk108623
- For a list of open issues, see the Known Limitations: sk108624 http://supportcontent.checkpoint.com/solutions?id=sk108624
- Visit the Check Point Exchange Point Community https://community.checkpoint.com/
  - Start discussions
  - Get answers from experts
  - Join the API community to get code samples and share yours
Upgrading to R80

The R80 Upgrade Verification Service helps you upgrade successfully to R80.

We evaluate your environment and send you an email that shows if you are ready to upgrade, or what you must do first. For more details, see sk110267 http://supportcontent.checkpoint.com/solutions?id=sk110267.

What's New

Unified Policy

Unified Console

SmartConsole applications are unified in R80, enabling administrators to control system aspects - including gateway configuration and monitoring and all log and event aspects.

- The Gateways & Servers tab enables the administrator to see a full view of the managed gateways, monitor their status and conduct maintenance operations.
- The Logs & Monitor tab enables the administrator to view and act on logs or events from the same console in which the security policies are configured.

Unified Security Policies

R80 offers unified policies for Access Control and Threat Prevention, enabling administrators to control several security aspects in a single policy.

- Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access Software Blade policies.
  Note - Supported only with R80.10 Security Gateways and Management.
- Threat Prevention policy unifies the IPS, Anti-Virus, Anti-Bot, and Threat Emulation Software Blade policies.
  Protections can be activated according to tags, enabling customers to activate relevant protections, such as protections related to a specific component (for example, Apache) or vulnerability type.

Policy Layers & Sub Policies

R80 introduces Policy Layers, enabling flexible control over the security policy behavior, and Sub Policies which enable seamless network segmentation within the security policy.

Note - Supported only with R80.10 Security Gateways and Management.

- The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence. If an "Accept" action was done in a layer, inspection will continue in the next layer.
- Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule. For example, a sub policy can manage a network segment or branch office.
• Sub Policies can be managed by specific administrators, according to their permissions profile, allowing easy responsibility delegation within the team.

Multi-Domain Security Management Enhancements
• Global policy and settings for blades.
• Unified architecture and unified client with single Domain security management.
• New and improved views for Domain provisioning and global configuration.

Efficient and Automated Operations

Role-based & Concurrent Administration
R80 enables several administrators to work in parallel on the same security policy, while offering a very granular and flexible privilege delegation to each administrator.
• Multiple administrators can log-in and work in read-write mode on the same security policy without interrupting each other’s work.
• A new advanced locking mechanism is introduced, enabling concurrent administration.
• Objects that one administrator manages can be locked from overwrites or conflicts by other administrators.
• Rich administrator profiles can determine the exact privileges each administrator will have, including management of specific policies or network segments, viewing specific logs, and conducting security operations, such as installing policy.

Secured Automation and Orchestration (CLI & API)
A complete CLI & API interface for security management enables full integration with 3rd party systems and automation of daily operations. Automation and SmartConsole management operations are allowed based on the same privilege profile.

Faster Day to Day Operations
R80 introduces multiple features that improve the work efficiency of administrators, such as:
• Integrated logging enables the administrator to view all logs related to a rule in the same screen.
• Detailed rule information is stored, providing visibility as to who created the rule and when, hit counts, and any other user defined information, such as ticket numbers.
• Enhanced search capabilities allow the administrator to immediately find any rule or object in the system.
• Management High Availability is enhanced to only sync changes between servers, significantly improving efficiency.
Integrated Threat Management

Next Generation Logs, Events and Reports

- Manage and monitor your security environment from a single, visual dashboard.
- Analyze hundreds of millions of logs per day.
- Rich graphical views and reports for security needs.
- Ability to customize views and reports to address specific requirements.
- Logging, monitoring, and report aspects of R80 SmartConsole are also available via web based interface.
- Free-text search of logs and events with auto-suggest and favorites - results in seconds.

New Licensing Experience

New license visibility and synchronization improve user experience.

Visibility mechanism:
- Improved visibility of Check Point’s Software Blade license status, alerts and User Center detailed information.
- Consolidated license status reports.

Synchronizing mechanism:
- Automatic activation for licenses on appliances.
- Seamless product license synchronization with Check Point’s User Center.
- Proxy configuration, enabling indirect User Center license synchronization for Check Point’s Gateways and Management Servers.

See Supported Blades for License Visibility for supported blades.

Improved Security for SIC and VPN certificates

SHA-256-based certificates are issued by default. For details, see sk103840 http://supportcontent.checkpoint.com/solutions?id=sk103840.

Build Numbers

Notes -
- Some of the Verifying Build Number commands show only the last three digits of the build number.
- The build numbers in the table below refer to R80 Take 132

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Build Number</th>
<th>Verifying Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaia</td>
<td>OS build 132</td>
<td>show version all</td>
</tr>
<tr>
<td>Security Management</td>
<td>Build 015</td>
<td>fwm ver</td>
</tr>
</tbody>
</table>
Upgrade Paths and Interoperability

R80 supports:

- Upgrades from earlier software versions with Database Migration. **Important!** To make sure you have the latest version of the upgrade tools, download the appropriate package from the Check Point Support site http://supportcontent.checkpoint.com/solutions?id=sk108623.
- Management of earlier Security Gateways with R80 management.

**Notes:**

- CPUSE and direct upgrade will be supported from R80.10.
- Upgrade is not supported from IPSO.

**Supported Upgrade Paths**

You can upgrade these Security Management Server and Multi-Domain Server versions to R80 with Database Migration:
R75.40, R75.45, R75.46, R75.47, R75.40 VS, R76, R77, R77.10, R77.20, and R77.30.

For R77.20 or R77.30 with the Add-on:

- It is not necessary to uninstall the Add-on.
- You must remove the unsupported features listed below or the upgrade to R80 will not be successful (the database export will fail).
- These features are not supported in R80:
  - Threat Extraction Software Blade.
  - Import of custom indicators to the Threat Prevention policy.
  - Modbus support with the Application Control Software Blade.
  - Support for Carrier solutions (LTE suite), such as NAT64, GTP, SCTP, CGNAT.
  - “SAML" Cloud Connector for web based single sign on.

---

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Build Number</th>
<th>Verifying Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartConsole</td>
<td>Build 991152104</td>
<td>Menu &gt; About Check Point SmartConsole</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>Build 003</td>
<td>fwm mds ver</td>
</tr>
<tr>
<td>Server Monitoring (SVM Server) Gaia</td>
<td>Build 072</td>
<td>rtm ver</td>
</tr>
</tbody>
</table>
Compatibility with Gateways

R80 Management Servers can manage gateways of these versions:

<table>
<thead>
<tr>
<th>Release</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Gateway</td>
<td>R75.20, R75.30, R75.40, R75.45, R75.40VS, R75.46, R75.47, R76, R77, R77.10, R77.20, R77.30</td>
</tr>
<tr>
<td>Security Gateway 80</td>
<td>R71.45, R75.20.x</td>
</tr>
<tr>
<td>1100 Appliance</td>
<td>R75.20.x, R77.20.x</td>
</tr>
<tr>
<td>1200R Appliance</td>
<td>R77.20.x</td>
</tr>
<tr>
<td>UTM-1 Edge</td>
<td>7.5.x and higher [Edge-X and Edge-W are not supported]</td>
</tr>
<tr>
<td>61000 Security System</td>
<td>61000 R75.035, 61000 R75.05x, R75.40VS for 61000, R76SP, R76SP.10, R76SP.20</td>
</tr>
<tr>
<td>VSX</td>
<td>R75.40 VS and higher</td>
</tr>
<tr>
<td>GX</td>
<td>5.0</td>
</tr>
<tr>
<td>Not supported</td>
<td>DLP-1, IPS-1, Connectra. GX 4.0</td>
</tr>
</tbody>
</table>

Supported Check Point Installations

All R80 servers are supported on the Gaia Operating System:

- Security Management Server
- Multi-Domain Security Management Server
- Log Server
- Multi-Domain Log Server
- SmartEvent Server

All R80 servers can be installed on VMware:

- Supported ESXi Server versions are: 4.0, 4.1, 5.0, 5.1, 5.5, 6.0
- Supported ESX versions are: 4.0, 4.1
Check Point Appliances

<table>
<thead>
<tr>
<th>Component</th>
<th>Security Management Server</th>
<th>Multi-Domain Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Single Socket 1x Core i5-3550S 4 cores, 3GHz or equivalent</td>
<td>Dual Socket 2x Xeon E5-2609v2 4 cores, 2.5GHz or equivalent</td>
</tr>
<tr>
<td>Total Cores</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Free Disk Space</td>
<td>500GB (Installation includes OS)</td>
<td>1TB (Installation includes OS)</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB RAM</td>
<td>32GB RAM</td>
</tr>
</tbody>
</table>
Gaia WebUI

The Gaia WebUI, also known as the Gaia Portal, is supported on these browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>14 and higher</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>8 and higher</td>
</tr>
<tr>
<td></td>
<td>(If you use Internet Explorer 8, file uploads through the Gaia Portal are limited to 2 GB.)</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>any</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>6 and higher</td>
</tr>
<tr>
<td>Safari</td>
<td>5 and higher</td>
</tr>
</tbody>
</table>

Supported Management Software Blades

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Gaia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy Management</td>
<td>✓</td>
</tr>
<tr>
<td>Logging &amp; Status</td>
<td>✓</td>
</tr>
<tr>
<td>Monitoring</td>
<td>✓</td>
</tr>
<tr>
<td>User Directory</td>
<td>✓</td>
</tr>
<tr>
<td>SmartEvent</td>
<td>✓</td>
</tr>
<tr>
<td>Compliance</td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Policy Management</td>
<td>✓*</td>
</tr>
</tbody>
</table>

Logging

Log Server Requirements

Logs can be stored:

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

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 R80.10 can connect to a different version of Log Server - R77.xx or earlier.

Usually SmartEvent and a Correlation Unit are 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.

Logging Capacity

<table>
<thead>
<tr>
<th>Check Point Appliance</th>
<th>Smart-1 205</th>
<th>Smart-1 210</th>
<th>Smart-1 225</th>
<th>Smart-1 3050</th>
<th>Smart-1 3150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexed logs per second</td>
<td>1,000</td>
<td>2,000</td>
<td>4,000</td>
<td>7,000</td>
<td>9,000</td>
</tr>
</tbody>
</table>

Notes

- The log rate is based on the peak traffic numbers. We assume that traffic about during regular operating hours are about half of these numbers. The published numbers are for dedicated Log Servers. For integrated Log and Management Servers, the numbers will be lower. See the *R80 Logging and Monitoring Guide* for more about logging.
- Performance and capacity for larger scale deployments will be fine-tuned and optimized during 2016. More detailed specifications will be published later this year.
Management Console

Console Hardware Requirements

This table shows the minimum hardware requirements for console applications:

<table>
<thead>
<tr>
<th>Component</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Pentium Processor E2140 or 2 GHz equivalent processor</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>2 GB</td>
</tr>
<tr>
<td>Video Adapter</td>
<td>Minimum resolution: 1024 x 768</td>
</tr>
</tbody>
</table>

Consoles by Windows Platform

SmartConsole is supported on:

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

Hardware Health Monitoring

R80 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 WebUI or SNMP to monitor fan speed, motherboard voltages, power supply health, and temperatures. Open Servers are only supported with an IPMI card.

<table>
<thead>
<tr>
<th>Check Point Appliances</th>
<th>Smart-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Hardware sensor monitoring (polling and traps)</td>
<td>✓</td>
</tr>
<tr>
<td>WebUI hardware sensor monitoring</td>
<td>✓</td>
</tr>
<tr>
<td>RAID monitoring with SNMP</td>
<td>✓</td>
</tr>
</tbody>
</table>

Open Servers

**Hardware Sensors Monitoring**: Use SNMP (polling and traps) or the WebUI to monitor hardware on IBM, HP, Dell, and Sun certified servers with an Intelligent Platform Management Interface (IPMI) card. The IPMI standard defines a set of interfaces to monitor system health.

.StringUtils"

Note - IPMI is an open standard. We cannot guarantee the Hardware Health Monitoring performance on all systems and configurations.
Changes in R80 Behavior

- The **Logging and Monitoring** view integrates SmartLog and replaces SmartView Tracker.
- SmartEvent replaces SmartReporter and SmartEvent Intro.

Known Limitations

See [sk108624](http://supportcontent.checkpoint.com/solutions?id=sk108624) for a complete list of known limitations that apply to this release.

These Software Blades are not supported in this release but will be addressed in the short term roadmap of releases after R80:

- SmartLSM and Provisioning.
- SmartWorkflow.

Licensing

Contact Account Services [mailto:accountservices@checkpoint.com?subject=Licensing Issues](mailto:accountservices@checkpoint.com?subject=Licensing Issues) for all license issues.