Check Point Compliance Blade
R75.40 and R75.45
Release Notes

Hotfix

20 May 2014
Important Info for the Compliance Blade

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.

Latest Documentation
The latest version of this document is at: (http://supportcontent.checkpoint.com/documentation_download?ID=23290)
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more information about this release, see the Compliance Blade Hotfix for R75.40 and R75.45 home page (http://supportcontent.checkpoint.com/solutions?id=sk92470).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 May 2014</td>
<td>Corrected path to Hotfix uninstallation executable for R75.40 (&quot;Uninstalling the R75.40 Hotfix&quot; on page 10) and R75.45 (&quot;Uninstalling the R75.45 Hotfix&quot; on page 10).</td>
</tr>
<tr>
<td>04 April 2013</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

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 Check Point Compliance Blade R75.40 and R75.45 Release Notes).
Contents

Important Info for the Compliance Blade ................................................................. 3
About the Check Point Compliance Blade ................................................................. 5
  Key Features ........................................................................................................... 5
  Security Best Practices ....................................................................................... 5
  Regulatory Compliance ....................................................................................... 5
  Supported Regulatory Standards ........................................................................ 5
  Continuous Compliance Monitoring ................................................................. 6
  Compliance Alerts ............................................................................................... 7
  Optimal Performance ......................................................................................... 7
  Check Point Compliance Blade Workflow ....................................................... 7
System Requirements ............................................................................................. 8
  Build Numbers .................................................................................................. 8
Installation and Uninstallation ................................................................................. 9
  Installing the R75.40 hotfix .............................................................................. 9
  Installing the R75.45 hotfix ............................................................................. 9
  Installing the SmartConsole Clients .................................................................. 10
  Uninstalling the R75.40 Hotfix ....................................................................... 10
  Uninstalling the R75.45 Hotfix ....................................................................... 10
Working with the Check Point Compliance Blade ............................................... 12
  The Overview Pane ............................................................................................ 13
  Security Best Practices Compliance ............................................................... 13
  Security Gateways ............................................................................................. 14
  Blades .................................................................................................................. 14
  Regulatory Compliance ...................................................................................... 14
  Messages and Action Items (SmartDashboard) ................................................. 15
  Searching, Grouping, Sorting .......................................................................... 15
  Working with Alerts and System Messages .................................................... 16
Working with Security Best Practices .................................................................... 17
  Activating Best Practice tests .......................................................................... 17
  Deactivating Security Best Practices ............................................................... 17
  Running a Manual Scan .................................................................................... 18
Working with Regulations ...................................................................................... 19
  Activating and Deactivating Regulations ....................................................... 19
Working with Action Items ................................................................................... 20
  Taking Corrective Action ................................................................................. 20
Running Reports ................................................................................................... 20
Exporting Data ...................................................................................................... 21
Chapter 1

About the Check Point Compliance Blade

In This Section:

- Key Features .......................................................... 5
- Check Point Compliance Blade Workflow ......................... 7

The Check Point Compliance Blade is a dynamic solution that continuously monitors the Check Point security infrastructure. This unique product examines your Security Gateways, Blades, Policies and configuration settings in real time. It compares them with an extensive database of regulatory standards and security best practices. The Check Point Compliance Blade includes many graphical displays and reports that show compliance with the applicable regulatory standards.

Key Features

Security Best Practices

The Check Point Compliance Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good gateway and Policy configuration. A Security Best Practice is related to specified regulations in different regulatory standards. It tells you about your compliance status and recommends corrective steps.

Types of Security Best Practices:

- **Global** - Examines the configuration settings for all of the organization.
- **Object-based** - Examines the configuration settings for specified objects (gateways, profiles and other objects).

Regulatory Compliance

The Check Point Compliance Blade monitors compliance with regulatory standards and shows their related Best Practices in an easy-to-read view. Each line shows the status, compliance score, and applicable Best Practices.

Supported Regulatory Standards

This Check Point Compliance Blade release supports these regulatory standards:

<table>
<thead>
<tr>
<th>Standard</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>International</td>
<td>Standards for the implementation of Information Security Management Systems (ISMS). This standard includes 133 control objectives that cover organizational security architecture.</td>
</tr>
<tr>
<td>ISO 27002</td>
<td>International</td>
<td>Supplemental controls and best practices for implementation of Information Security Management Systems (ISMS). This standard includes detailed control objectives that are applicable to certain industries.</td>
</tr>
<tr>
<td>Standard</td>
<td>Location</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HIPAA Security</td>
<td>USA</td>
<td>Health Insurance Portability and Accountability Act of 1996. These regulations require government agencies, insurers and health care providers to protect all data that they collect, maintain or use.</td>
</tr>
<tr>
<td>PCI DSS 2.0</td>
<td>USA</td>
<td>Industry standards for transmission, processing and storage of credit card data.</td>
</tr>
<tr>
<td>DSD</td>
<td>Australia</td>
<td>Military data security regulations and standards</td>
</tr>
<tr>
<td>GLBA</td>
<td>USA</td>
<td>Gramm-Leach-Bliley Act. These regulations include financial privacy guidelines and safeguards related to information security.</td>
</tr>
<tr>
<td>NIST 800-41</td>
<td>USA</td>
<td>National Institute of Standards and Technology guidelines for firewalls and Firewall Policies</td>
</tr>
<tr>
<td>NIST 800-53</td>
<td>USA</td>
<td>National Institute of Standards and Technology recommend security controls for federal government information systems and organizations.</td>
</tr>
<tr>
<td>FIPS 200</td>
<td>USA</td>
<td>FISMA regulations that require federal agencies to comply with the recommended security controls as specified in NIST 800-53.</td>
</tr>
<tr>
<td>UK Data Protection Act</td>
<td>UK</td>
<td>British data security standards that include eight data protection principles.</td>
</tr>
<tr>
<td>CobiT 4.1</td>
<td>USA</td>
<td>34 information technology governance framework that includes control requirements, technical issues and business risks.</td>
</tr>
<tr>
<td>SOX</td>
<td>USA</td>
<td>Additional information technology controls defined in the CobiT framework that includes control requirements, technical issues and business risks.</td>
</tr>
<tr>
<td>MAS TRM</td>
<td>Singapore</td>
<td>Technology risk management for financial institutions in Singapore. This standard includes 202 regulatory requirements in 12 areas.</td>
</tr>
<tr>
<td>GPG13</td>
<td>UK</td>
<td>Good Practices Guide 13, published by the British Government includes 12 Protective Monitoring Controls (PMCs). The controls are a set of technology processes to improve company profiles.</td>
</tr>
<tr>
<td>NERC</td>
<td>US &amp; Canada</td>
<td>North American Electric Reliability Corporation guidelines for critical infrastructure protection. This document includes nine standards that cover everything from security management controls to system security.</td>
</tr>
</tbody>
</table>

**Continuous Compliance Monitoring**

Continuous Compliance Monitoring (CCM) is a dynamic technology that continuously examines compliance parameters. The Check Point Compliance Blade uses CCM to examine Security Gateways and the security Policies with this schedule:

- **SmartDashboard changes** - Automatic scan when an administrator changes objects that have an effect on gateway or Policy configuration.
- **Daily** - Automatic scan one time each day, finds changes to gateway and Policy configurations made with CLI or scripts.

You can also run manual scans as necessary.
Compliance Alerts
If administrator actions cause a degradation of the compliance status, the Check Point Compliance Blade shows an alert with details of the issue. It also generates an action item to monitor corrective steps.

Optimal Performance
The Check Point Compliance Blade does not cause degradation of network throughput or client performance.

Check Point Compliance Blade Workflow
This is the recommended workflow for the Check Point Compliance Blade:
1. View - Use the Check Point Compliance Blade tools to examine and monitor compliance status.
2. Plan - Use automatically generated Action Items to make a plan to take corrective action.
3. Act - Correct compliance issues as recommended by the Action Items. You can see the updated compliance status after you run Check Point Compliance Blade scans.
System Requirements

You can use this Check Point Compliance Blade release with these versions:

- R75.40 (http://downloads.checkpoint.com/dc/download.htm?ID=13079)
- R75.45 (http://downloads.checkpoint.com/dc/download.htm?ID=18381)

The system requirements for this hotfix are the same as described in the release notes for these versions. You cannot upgrade to higher versions with this hotfix. If you do this, the Check Point Compliance Blade is not available.

Build Numbers

R75.40

This table shows the R75.40 software products updated in this release and their build numbers. All other build numbers are the same as in R75.40 (http://downloads.checkpoint.com/dc/download.htm?ID=13079).

To confirm that the hotfix is installed, run the version command for each product.

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Build Number</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management</td>
<td>TBD</td>
<td>fwm ver</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>986001006</td>
<td>fwm mds ver</td>
</tr>
</tbody>
</table>

You must install an upgraded SmartConsole after you install the management server and gateways.

<table>
<thead>
<tr>
<th>SmartConsole Applications</th>
<th>Build Number</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>986028078</td>
<td>Help &gt; About Check Point &lt;Client Application&gt;</td>
<td></td>
</tr>
</tbody>
</table>

R75.45

This table contains the R75.45 software products updated in this release and their build numbers. All other build numbers are the same as in R75.45 (http://downloads.checkpoint.com/dc/download.htm?ID=18381).

To confirm that the hotfix is installed, run the version command for each product.

<table>
<thead>
<tr>
<th>Software Blade / Product</th>
<th>Build Number</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management</td>
<td>TBD</td>
<td>fwm ver</td>
</tr>
<tr>
<td>Multi-Domain Server</td>
<td>986092004</td>
<td>fwm mds ver</td>
</tr>
</tbody>
</table>

You must install an upgraded SmartConsole after you install the management server and gateways.

<table>
<thead>
<tr>
<th>SmartConsole Applications</th>
<th>Build Number</th>
<th>Version Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>986650048</td>
<td>Help &gt; About Check Point &lt;Client Application&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Installation and Uninstallation

The procedure for installing the hotfix on the management server is different for R75.40 and R75.45

Installing the R75.40 hotfix

To install the hotfix on SecurePlatform or Gaia:
2. Put the installation package in a temporary directory on the management server.
3. From the temporary directory, run `tar -zxvf R75.40_GRC_LINUX.tgz`.
4. Run `.\UnixInstallScript` and do the instructions on the screen.
5. When the `Succeeded` message shows, enter 'y' to restart the server.

To install the hotfix on Windows:
2. Put the installation package in a temporary directory on the management server.
3. Extract the installation executable.
4. Run `Setup.exe` and do the instructions on the screen.
5. When the `Succeeded` message shows, click 'y' to restart the server.

To install the hotfix on a Multi-Domain Security Management Multi-Domain Server:
2. Put the installation package in a temporary directory on the Multi-Domain Server.
3. From the temporary directory, run `tar -zxvf R75.40_GRC_LINUX.tgz`.
4. Run `.\UnixInstallScript` and do the instructions on the screen.
5. When the `Succeeded` message shows, enter 'y' to restart the server.
6. In the SmartDomain Manager, go to Updates > Version & Blade Updates.
7. Activate the hotfix for each Domain:
   a) Right-click the Domain.
   b) Select Activate Update on this Domain.
      You must wait for the update to complete before you activate a different Domain.

Installing the R75.45 hotfix

To install the hotfix on SecurePlatform Gaia:
2. Put the installation package in a temporary directory on the management server.
3. From the temporary directory, run `tar -zxvf R75.45_GRC_LINUX.tgz`.
4. Run `.\UnixInstallScript` and do the instructions on the screen.
5. When the `Succeeded` message shows, enter 'y' to restart the server.

To install the hotfix on Windows:
2. Put the installation package in a temporary directory on the management server.
3. Extract the installation executable.
4. Run Setup.exe and do the instructions on the screen.
5. When the Succeeded message shows, click 'y' to restart the server.

To install the hotfix on a Multi-Domain Security Management Multi-Domain Server:
2. Put the installation package in a temporary directory on the Multi-Domain Server.
3. Run tar -zxvf R75.45_GRC_Linux.tgz.
4. From the temporary directory, run ./UnixInstallScript and do the instructions on the screen.
5. When the Succeeded message shows, enter 'y' to restart the server.
6. In the SmartDomain Manager, go to Updates > Version & Blade Updates.
7. Activate the hotfix for each Domain:
   a) Right-click the Domain.
   b) Select Activate Update on this Domain.
      You must wait for the update to complete before you activate a different Domain.

Installing the SmartConsole Clients

To Install the SmartConsole clients:
2. Right-click Setup.exe and select Run as administrator.
3. Do the instructions on the screen.

Uninstalling the R75.40 Hotfix

To uninstall the hotfix on SecurePlatform or Gaia:
1. Go to /opt/CPUninstall/R75.40_Compliance.
2. Run ./UnixUninstallScript and do the instructions on the screen.

To uninstall the hotfix on Windows:
1. Run:
   c:\Program Files\CheckPoint\CPuninstall\R75.40_Compliance\MiniWrapper.exe -uninstall.
2. Do the instructions on the screen.

To uninstall the hotfix on a Multi-Domain Security Management Multi-Domain Server:
1. Go to /opt/CPUninstall/R75.40_Compliance.
2. Run ./UnixUninstallScript and do the instructions on the screen.
3. In the SmartDomain Manager, go to Updates > Version & Blade Updates.
4. Deactivate the hotfix for each Domain:
   a) Right-click the Domain.
   b) Select Deactivate Update on this Domain.
      You must wait for the update to complete before you deactivate a different Domain.

Uninstalling the R75.45 Hotfix

To uninstall the hotfix on SecurePlatform or Gaia:
1. Go to /opt/CPUninstall/R75.45_Compliance.
2. Run ./UnixUninstallScript and do the instructions on the screen.
To uninstall the hotfix on Windows:
1. Run:
   `c:\Program Files\CheckPoint\CPUninstall\R75.45_Compliance\MiniWrapper.exe -uninstall`.
2. Do the instructions on the screen.

To uninstall the hotfix on a Multi-Domain Security Management Multi-Domain Server:
1. Go to `/opt/CPUninstall/R75.45_Compliance`.
2. Run `./UnixUninstallScript` and do the instructions on the screen.
3. In the SmartDomain Manager, go to Updates > Version & Blade Updates.
4. Deactivate the hotfix for each Domain:
   a) Right-click the Domain.
   b) Select Deactivate Update on this Domain.
      You must wait for the update to complete before you deactivate a different Domain.
Chapter 2

Working with the Check Point Compliance Blade

In This Section:
The Overview Pane ................................................................. 13
Searching, Grouping, Sorting.............................................. 15
Working with Alerts and System Messages........................... 16

The Overview pane shows the overall compliance status of your organization. Select the different branches in the navigation tree to see more details.

To work with the Check Point Compliance Blade in SmartDashboard, go to the Compliance tab in SmartDashboard.
To work with the Check Point Compliance Blade in Multi-Domain Security Management, go to the Compliance tab in SmartDomain Manager (R77.20 and Higher).

### The Overview Pane

The Overview pane shows:

<table>
<thead>
<tr>
<th>Element</th>
<th>What can I do here?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Best Practices Compliance</td>
<td>See the compliance distribution by Security Best Practice status</td>
</tr>
<tr>
<td>Security Status by Gateways</td>
<td>See compliance scores for selected Security Gateways</td>
</tr>
<tr>
<td>Security Status by Blade</td>
<td>See compliance scores and Security Best Practices by blade</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>See a summary of compliance with different regulations</td>
</tr>
<tr>
<td>Action Items and Messages</td>
<td>See action items, compliance alerts, and system messages</td>
</tr>
</tbody>
</table>

### Security Best Practices Compliance


The Check Point Compliance Blade includes many predefined Security Best Practices. In versions R77.20 and higher you can define your own custom Security Best Practices.

The Check Point Compliance Blade calculates a numeric score for each Security Best Practice, which is the average of the results for each object examined. Scores can show for the organization, Security Gateways, Software Blades, and regulations.

This is the Check Point Compliance Blade scoring system:
A category can show **N/A** scores if:

- The Software Blade is not installed on the Security Management Server
- The Security Gateway does not support the examined feature
- You created a new Security Best Practice, but did not do a manual scan.
- A Security Best Practice is not activated for your organization
- A Security Best Practice cannot run because it is dependent on another Security Best Practice with a non-compliant status

Many Security Best Practices are binary: compliant or not.

- Low = 0
- Secure = 100

Other Security Best Practices calculate a score based on the degree of security compliance.

### Security Gateways

This SmartDashboard pane shows Security Gateways and Security Gateway Clusters with the highest compliance scores, lowest compliance scores, or a predefined set of **Favorites**.

- To see the Security Best Practice results for a Security Gateway, select it. The Gateways pane for the selected gateway opens.
- To see the results for all gateways, click **See All Gateways**. The **All Gateways** window opens.

### Blades

This pane shows the average scores for the five Software Blades with the most Security Best Practices. The results show in descending order by the number of Security Best Practices. To see Security Best Practice results for one Software Blade, click that blade. The **Security Best Practices** pane opens.

To see the results for all Software Blades, click **More Details**. The **Security Best Practices** pane opens. Group the results by **Blade**.

### Regulatory Compliance

The Check Point Compliance Blade includes many predefined governmental and industry standards right out of the box. From release 77.20 and higher, you can also define Regulations and Regulatory standards. This functionality is useful to manage organizational or local regulatory agency requirements.

The **Regulatory Compliance** pane shows compliance statistics for selected regulatory standards, based on the Security Best Practice scan. This pane shows:

- The total number of Regulatory Requirements that are monitored
- The Number of Regulatory Requirements for each Regulation
- The Average compliance score for each regulation shown

The number of regulatory standards shown is based on your screen resolution.
To select the regulatory standards to show:
1. Click the configuration icon in the top right corner of the pane.
2. In the Select Regulations and Standards window, select the standards to show in the Overview.

Note - If a regulatory standard is not selected in the Settings window, it is does not show in this widget.

To see the compliance score for all Regulatory Requirements, click See all Regulations. The All Regulatory Requirements window opens.

To see details of a standard, click the name of the standard in the Overview pane or in the All Regulatory Requirements window. The Regulatory Requirements pane for the selected standard opens.

**Messages and Action Items (SmartDashboard)**

This pane shows the updated status of pending action items for your organization.

- **Overdue** - Action items that are overdue.
- **Upcoming** - Action items with due dates in the next 30 days.
- **Future** - Action items with due dates of more than 30 days.
- **Unscheduled** - Action items without defined due dates.

Note: We recommend that you resolve overdue action items immediately.

If you have a high resolution screen, the Alert and System messages show in the bottom section of the pane. Use the arrows to scroll through the messages.

If you have a low resolution screen, two buttons show in the bottom section of the pane.

- To see alert messages, click Security Alerts. They open in the Overview pane.
- To see messages about the Check Point Compliance Blade, click System Messages. They open in the Overview pane.

**Searching, Grouping, Sorting**

In the Check Point Compliance Blade panes, enter a string in the search field to filter results.
To search for values in a field, enter: `field_name:string`

To combine results into groups, select **Blade** or **Status** in the grouping field.

To sort the results by values in field, click that field header.

### Working with Alerts and System Messages

You use the **Security Alerts and System Message** pane to see Security Alerts generated when a configuration change causes compliance status degradation. You can also see messages that are automatically generated by the Check Point Compliance Blade.

To see the details of a system message, double-click it. The **Security Alert Details** window opens.
Chapter 3

Working with Security Best Practices

In This Section:

Activating Best Practice tests
Deactivating Security Best Practices
Running a Manual Scan

You can activate or deactivate Security Best Practice enforcement for the entire organization or by specified object. Activation changes are applied after the next security scan. All Security Best Practices are activated by default. You can deactivate and reactivate Security Best Practices as necessary.

Activating Best Practice tests

By default all Best Practice tests are active.

To activate a Best Practice test that is not currently active:
1. Select a Best Practice test in the top section or in the Related Objects section.
2. Select Active.

Deactivating Security Best Practices

You can deactivate Security Best Practices globally for the organization or for specified objects (gateways, blades or profiles).

To deactivate a Security Best Practice for all of the organization:
2. When prompted, enter an explanation.
   A comment is required to show why it is necessary to stop running this Security Best Practice.
3. Optional: Define an expiration date.
   If you define an expiration date, the deactivated Security Best Practice is automatically reactivated on that date.

To reactivate a Security Best Practice:

1. Open Settings > Inactive Objects.
2. Select a Security Best Practice from the list.
3. Click Delete.
   (Or select the Active option in the Security Best Practices pane.)

**To change the comment or expiration date:**
Double-click a Security Best Practice in the Inactive Objects pane.

**To deactivate Security Best Practices for specified gateways:**
1. Open Settings > Inactive Objects.
2. In the Inactive Gateways section, click Add.
3. Enter or select a gateway or cluster.
   The selected gateways show in the Inactive Gateways list.

**To remove a gateway from the Inactive Gateways list:**
1. Select the gateway.
2. Click Remove.
3. When prompted, click Yes.

**To deactivate a Security Best Practice for a specified object:**
2. In the Relevant Objects section, clear the Active option for the object.
   An object can be a gateway, Policy, profile or other object.
3. When prompted, enter an explanation.
   A comment is required to show why it is necessary to stop running this Security Best Practice.
4. Optional: Define an expiration date.
   If you define an expiration date, the deactivated Security Best Practice is automatically reactivated on that date.

**To reactivate an object for Security Best Practices:**
1. Open Settings > Inactive Objects.
   The de-activated Security Best Practice is in the Inactive Security Best Practices on Specific Objects section.
2. Select the Security Best Practice.
3. Click Delete.
   (Or select the Active option in Security Best Practices > Relevant Objects of the selected Security Best Practice.)

---

**Running a Manual Scan**

We recommend that you run a manual scan after:
- You add objects to your Check Point environment.
- You make changes to IPS protections. Changes to IPS protections are not automatically updated.
- You activate or de-activate a Security Best Practice.

**To run a manual scan:**
1. Open the Compliance tab.
2. In the Navigation tree, select Settings.
3. On the Settings page, click Rescan.
   **Note:** While a scan is running, you cannot work with the Compliance tab.
Chapter 4

Working with Regulations

In This Section:

Activating and Deactivating Regulations ................................................................. 19

The Regulations pane shows the status of Security Best Practices related to regulatory standards.

To work with regulations and their status:
1. On the Compliance tab, click Regulatory Requirements.
2. Select a regulatory standard.

The selected regulatory standard pane opens.

The top table shows the status of pending Action Items:
- **ID** - ID of the related Security Best Practice.
- **Status** - Low, Medium, High, Compliant, or N/A.
  We recommend that you resolve Low status items immediately.
- **Name** - Name and brief description of the Security Best Practice.

The bottom section shows information about the selected regulations:
- **Relevant Objects** - Objects related to the selected Security Best Practice and their status. (Shows when the selected Security Best Practice applies to specified objects.)

Activating and Deactivating Regulations

You can select the regulatory standards that are applicable to your organization. By default, all supported regulatory standards are active.

To activate or deactivate regulatory standards:
1. In the navigation tree, click Settings.
2. Select the regulatory standards that are applicable for your organization.
3. Clear the regulatory standards that are not applicable for your organization.
Chapter 5

Working with Action Items

In This Section:

Taking Corrective Action........................................................................................................................................ 20

When a Security Best Practice finds a violation, the Check Point Compliance Blade automatically generates an Action Item. You can assign a due date to an Action Item and monitor corrective steps. By default, Action Items do not have a due date. When you complete the corrective steps, the Check Point Compliance Blade deletes the Action Item after the next scan.

To assign a due date for an Action Item:
1. Open Messages and Action Items > Action Items.
2. Select an Action Item.
3. In the Action Item Description section, click Schedule Now.
   If the Action Item already has an assigned due date, click Change to change it.
4. In the window that opens, enter or select a due date and then click OK.

To delete an action item:
2. Run a manual scan: Settings > Rescan.

Taking Corrective Action

The Action Items pane shows a helpful description for each Action Item, which gives suggestions to correct the related configuration settings. You can correct many issues quickly and easily. For some objects, you can double-click the object in the Relevant Objects section to open its configuration window in SmartDashboard.

You can also correct some issues from the command line. If an Action Item does not have a link to an object, use the description to guide you through the configuration steps.

Running Reports


- Security Overview - Shows the summary data included in the Overview pane:
  - Summaries of gateways
  - Summaries of regulatory standards
  - Detailed lists of Security Best Practices
  - Action items.
- By Regulation - Shows a summary of the Regulatory Requirements and a detailed list of the Security Best Practices included in each requirement.

To generate a report, select Reports on the Navigation tree and then select a report. The report shows in a pane with the report name as the title.

From the report pane, you can create reports in these output formats:
You can copy data in a Check Point Compliance Blade table and paste it to other applications, such as spreadsheets, word processors, and text editors. This lets you save data for analysis and audits. You can select and copy one row, a group of rows or all of the rows in a table.

**To copy one row or a group of rows:**
1. Select one or more rows.
2. Right-click the rows and select *Copy to Clipboard* from the Options menu.
3. Paste the data into your application.

**To copy all rows in a table:**
1. Right-click inside the table and select *Select All* from the Options menu.
2. Right-click again and select *Copy to Clipboard* from the Options menu.
3. Paste the data into your application.