

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

# **R70.30**

## **Installation and Upgrade Guide**

## More Information

The latest version of this document is at:

[http://supportcontent.checkpoint.com/documentation\\_download?ID=10658](http://supportcontent.checkpoint.com/documentation_download?ID=10658)

For additional technical information about Check Point visit 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 to us ([mailto:cp\\_techpub\\_feedback@checkpoint.com?subject=Feedback on R70.30 Installation and Upgrade Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R70.30 Installation and Upgrade Guide)).

## © 2010 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:

Please refer to our Copyright page (<http://www.checkpoint.com/copyright.html>) for a list of our trademarks.

Please refer to our Third Party copyright notices ([http://www.checkpoint.com/3rd\\_party\\_copyright.html](http://www.checkpoint.com/3rd_party_copyright.html)) for a list of relevant copyrights.

# Contents

---

<b>Introduction</b> .....	<b>4</b>
<b>Deployment Planning</b> .....	<b>5</b>
Event Correlation & Reporting Planning .....	5
IPS Event Analysis Planning .....	5
<b>Installing R70.30</b> .....	<b>7</b>
New Installation .....	7
Upgrading from R70, R70.1 or R70.20 .....	7
Updating Customized INSPECT Files .....	7
Installation Using the Web User Interface .....	8
Installation Using the Command Line.....	9
Installation Using the Command Line - IPSO Flash-Based .....	10
Installation using SmartUpdate .....	11
Upgrading from NGX R60 - R65 .....	12
Installing the Client Applications .....	13
Starting SmartDashboard for the First Time.....	13
Your First Session .....	14
<b>Initial Configuration</b> .....	<b>15</b>
Configuring Event Correlation & Reporting .....	15
Standalone Deployment.....	15
Distributed Deployment.....	16
Provider-1 Deployment .....	17
Configuring IPS Event Analysis .....	19
Standalone Deployment.....	19
Distributed Deployment.....	19
Provider-1 Deployment .....	20
Configuring SmartWorkflow .....	21
Assigning Permissions.....	21
Enabling the SmartWorkflow Blade.....	22
Configuring SmartWorkflow Properties .....	24
<b>Uninstalling R70.30</b> .....	<b>26</b>
<b>Index</b> .....	<b>27</b>

# Chapter 1

---

## Introduction

Thank you for updating to R70.30. This release is a recommended update that contains new features and resolves various issues for the Check Point products.

Please read this document carefully prior to installing R70.30.

For more information about this release, see the *R70.30 Release Notes* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10694](http://supportcontent.checkpoint.com/documentation_download?ID=10694)).

# Chapter 2

---

## Deployment Planning



**Note** - Read this chapter if you have upgraded from R70 or R70.1, or if you have upgraded from R70.20 but not yet deployed Event correlation and IPS Event Analysis

This chapter contains information regarding planning your deployment for the Event Correlation and IPS Event Analysis software blades.

### In This Chapter

<a href="#">Event Correlation &amp; Reporting Planning</a>	5
<a href="#">IPS Event Analysis Planning</a>	5

## Event Correlation & Reporting Planning

The Event Correlation Blade is based on two components: an Eventia Analyzer server, and an Eventia Correlation unit. The Reporting Blade is based on the Eventia Reporter server. All three components can reside on a Security Management server or dedicated Log server. You can also install some components on a Security Management server and some components on a dedicated Log server, in order to distribute the load. In a Provider-1 deployment, the three components must be installed on one or more dedicated Log servers, and not on the Provider-1 MDS.

**Important:** Regardless of where the various components reside, the R70.30 release package must be installed on all management servers in your deployment, including Security Management servers, Provider-1 MDSs, MLMs, log servers (including log servers that host earlier releases of Eventia Analyzer and Eventia Reporter).



**Note** - You can install the R70.30 release package on IPSO and Solaris. However, IPSO and Solaris are not supported for use as an IPS Event Analysis server, Eventia Analyzer server, Event Correlation unit, or Eventia Reporter server.

## IPS Event Analysis Planning

IPS Event Analysis is based on two components: the IPS Event Analysis server and the IPS Correlation unit. Both components can be installed on the same or separate computers. The default configuration and recommended deployment is that each Log server is used as an IPS Correlation Unit, and that the IPS Event Analysis server resides on the R70 Security Management server or dedicated R70 Log server, according to the expected load.

The components can be installed according to the following deployments:

Deployment	Configure IPS Event Analysis Server on	Configure IPS Event Correlation on
All-in-one	Security Management server	Security Management server (that is also a Log server)

Deployment	Configure IPS Event Analysis Server on	Configure IPS Event Correlation on
Basic Load 1	Security Management server	Dedicated Log server
Basic Load 2	Dedicated Log server	Security Management server (that is also a Log server)
Moderate Load/ Provider-1	Dedicated Log server	Same dedicated Log server
Heavy Load/ Provider-1	Dedicated Log server	Additional dedicated Log server(s)

Important: Regardless of where the IPS Event Analysis servers reside, the R70.30 release package must be installed on all management servers in a deployment, including Security Management servers, Provider-1 MDSs, MLMs, Log servers, Eventia Reporter servers, and Eventia Analyzer servers.



**Note** - You can install the R70.30 release package on IPSO and Solaris. However, IPSO and Solaris are not supported for use as an IPS Event Analysis server, Eventia Analyzer server, Event Correlation unit, or Eventia Reporter server.

The IPS Event Correlation process produces events by processing the logs from the Log server against the Event Policy. The IPS Event Analysis server runs a database that is populated by events that result from the IPS Event Correlation process.

# Chapter 3

---

## Installing R70.30

### In This Chapter

<a href="#">New Installation</a>	7
<a href="#">Upgrading from R70, R70.1 or R70.20</a>	7
<a href="#">Upgrading from NGX R60 - R65</a>	12
<a href="#">Installing the Client Applications</a>	13
<a href="#">Starting SmartDashboard for the First Time</a>	13

## New Installation

R70.30 is released as an upgrade to versions R70 and higher. If you are installing R70.30 as a new installation on any management server, gateway or log server, you must first install version R70 as described in the R70 Installation and Upgrade Guide ([http://supportcontent.checkpoint.com/documentation\\_download?ID=8753](http://supportcontent.checkpoint.com/documentation_download?ID=8753)). In this case, we suggest that you also install Eventia Suite version R70 during this process. Once you have successfully completed the R70 installation, you then install the release package as an upgrade from R70 to R70.30.

If you have previously installed R70 without the Eventia Suite, it is not necessary to install at this time. The R70.30 installation package will install these applications automatically. You must, however, enable and configure the various components. For details, see the R70.30 Installation and Upgrade Guide ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10658](http://supportcontent.checkpoint.com/documentation_download?ID=10658)).

Some of the steps in the configuration process may apply only to newly installed servers. You can safely skip these steps.

## Upgrading from R70, R70.1 or R70.20

This section presents the procedures for installing R70.30 on management servers, gateways and log servers.

- If you do not already have version R70 or higher installed on your computers, perform a fresh installation or upgrade your system as described in the *R70 Installation and Upgrade Guide* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=8753](http://supportcontent.checkpoint.com/documentation_download?ID=8753)).
- If you are upgrading from pre-R70 versions of Eventia Analyzer and Eventia Reporter, you should first upgrade them to R70 and only then continue installing this version.

We recommend that you backup your system before installing this release package. For SecurePlatform, you can use snapshots which are discussed in the Snapshot Image Management section of the *R70 SecurePlatform/SecurePlatform Pro Administration Guide* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=8744](http://supportcontent.checkpoint.com/documentation_download?ID=8744)).

## Updating Customized INSPECT Files

The management server hosts several INSPECT (\*.def) files, typically located in the **\$FWDIR/lib** directory. This release may include one or more updated INSPECT files, which will replace the INSPECT files currently in use. For environments using only original Check Point INSPECT files, the updated INSPECT files are installed automatically. No user intervention is required.

If you have manually customized any INSPECT file was, **none** of the new INSPECT files will replace the previous ones. The following message appears:

```
The updated inspect files were NOT installed due to signature mismatches or errors.
To complete the installation replace the inspect files.
Inspect files that were not replaced may lead to unexpected behavior!
To force update of the inspect files run: update_inspect_files -f
```

If the INSPECT files are not replaced (signature mismatch message displayed), you must force an update of **all** INSPECT files to (whether or not manually customized).



**Important** - You must replace the previous versions of the INSPECT files. If you fail to do so, unexpected behavior may result.

### To force update of all INSPECT files:

1. Make note of the customized INSPECT files.

To see which INSPECT files were not replaced, refer to the logs:

- **Unix** - /opt/CPInstLog/update\_inspect\_files\_60.log
- **Windows** - C:\Program Files\CheckPoint\CPInstLog\update\_inspect\_files\_60.log

If the files were not replaced due to manual customization, the log displays:

```
<filename>.def was changed by user, signature didn't match!
```

2. Open those files listed in update\_inspect\_files\_60.log. Note the customized lines.
3. Run: update\_inspect\_files -f. The log will show <filename>.def was replaced.
4. Merge the customized content (that you noted in the previous steps) into the new INSPECT file(s).
5. Re-install the Security Policy to enable the new INSPECT files.

## Installation Using the Web User Interface

You can install R70.30 on SecurePlatform and supported Check Point appliances using the SecurePlatform Web User interface.

### To install on SecurePlatform using the Web User Interface:

1. Download Check\_Point\_R70.30.linux.tgz ([http://supportcenter.checkpoint.com/file\\_download?id=10734](http://supportcenter.checkpoint.com/file_download?id=10734)) from the Check Point Download Center.
2. Connect to the SecurePlatform WebUI at: `https://<IP_address>`.  
For appliances, connect to the SecurePlatform WebUI at: `https://<IP_address>:4434`.
3. From the **Upgrade** page select **Device > Upgrade**.

#### Upgrade Steps

To upgrade your device, please follow the next steps:

1. Download an upgrade package from [Check Point Download Center](#)  

Note: if you already downloaded the file you can skip this step.
2. Select the upgrade package file
3.
4. **Safe Upgrade**

Save a snapshot of the current system before the upgrade.  
If the upgrade fails - automatically revert to that snapshot.

**Double-Safe Upgrade**

Require a successful login connection within  minutes after the upgrade.  
If no login happens - automatically revert to the saved snapshot.

Note: Your browser will automatically try to perform the first login immediately after the upgrade. To enable that, you should not close this window and should not browse to any other page. Otherwise, you will have to login manually before the above interval expires.
5.  Package currently found on device

4. Click **Browse** and navigate to the installation package file downloaded in step 1.
5. Click **Upload package to device**.
6. Optionally select one of the Safe Upgrade options.
7. Click **Start Upgrade**.

## Installation Using the Command Line

This section provides the general instruction for installing this version from the command line on all supported management servers, gateways and log servers except IPSO flash-based appliances ("[Installation Using the Command Line - IPSO Flash-Based](#)" on page 10).

Before installing, verify that the target computer platform is supported, as stated in *R70.30 Release Notes*. ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10694](http://supportcontent.checkpoint.com/documentation_download?ID=10694))

Installation on IPSO platforms using Network Voyager is not supported and may result in system instability. You must install using the CLI only.

### To install this release :

1. Log onto the target machine.
2. If you are installing on SecurePlatform, run `idle 120`. This step ensures that installation is not interrupted by the automatic logon timeout.
3. Enter the expert mode.
4. Verify that the target computer contains sufficient free disk space, as stated in *R70.30 Release Notes*. ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10694](http://supportcontent.checkpoint.com/documentation_download?ID=10694))
5. Create a temporary directory under `/var` on the target computer.
6. Download the appropriate files from the Check Point Download Center.

Platform	File Name
SecurePlatform or Linux	Check_Point_R70.30.linux.tgz ( <a href="http://supportcenter.checkpoint.com/file_download?id=10734">http://supportcenter.checkpoint.com/file_download?id=10734</a> )
Solaris	Check_Point_R70.30.solaris2.tgz ( <a href="http://supportcenter.checkpoint.com/file_download?id=10735">http://supportcenter.checkpoint.com/file_download?id=10735</a> )
IPSO Disk-based	Check_Point_R70.30.ipso6.tgz ( <a href="http://supportcenter.checkpoint.com/file_download?id=10737">http://supportcenter.checkpoint.com/file_download?id=10737</a> )
Windows	Check_Point_R70.30.windows.tgz ( <a href="http://supportcenter.checkpoint.com/file_download?id=10736">http://supportcenter.checkpoint.com/file_download?id=10736</a> )

7. Copy the file to the temporary directory using SFTP, SCP, or other secure method.
8. Navigate to the temporary directory and extract the .tgz package
  - On non-Windows platforms, run `gtar -zxvf <file name>`
  - On Windows platforms, use an archive utility, such as WinZip.



**Note** - You can safely delete the .tgz file once it has been extracted.

9. Start the installation routine,
  - Run `./UnixInstallScript` on non-Windows platforms.
  - Run `setup.bat` on Windows platforms.
10. Follow the instructions on the screen to install the appropriate components. Only those components required for a specific target (management or gateway) are installed automatically. When the installation finishes, each successfully installed component appears in a list followed by the word '**Succeeded**'.
11. When prompted, reboot the computer.
12. Repeat the above steps for all management servers, log servers and gateways as required by your deployment.
13. After completing the installation on all computers, install the security policy on gateways and servers as appropriate.

## Installation Using the Command Line - IPSO Flash-Based

- Before attempting to upgrade your diskless IPSO platform, verify that the target computer platform is supported, and the disk space requirements, as stated in *R70.30 Release Notes*. ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10694](http://supportcontent.checkpoint.com/documentation_download?ID=10694))
- IPSO Diskless platforms are supported for use as Security Gateways only.
- Installation using Network Voyager is not supported and may result in system instability. You must install this version using the CLI only.

### Before installing on an IPSO Diskless Appliance

1. Delete any Check Point packages that are earlier than R70, and then delete any previous tgz files. You can do this using Network Voyager or using the command shell:

Using Network Voyager:

- Choose **Configuration > System Configuration > Packages > Delete Packages**.
- Select a previous installation package to delete, and click **Apply**.
- Delete the any tgz files.
- Click **Apply**.

Using the command shell, run the following commands:

```
newpkg -q
newpkg -u <previous package name>
rm opt/packages/<previous tgz name>
```

2. If there is an IPSO 4.x image on the machine, delete it using Network Voyager:
  - Choose **Configuration > System Configuration > images > Manage Images**.
  - Click **Delete IPSO Images**.
  - Select the IPSO 4.x image to delete, and click **Apply**.
3. Verify that there is enough free disk space for the installation of the packages:
  - For `/preserve`, you need at least 455000 KB free.  
(To find absolute free space: run the `df -k /preserve` command and subtract the 3rd column `Used` from the 2nd column `1K-blocks`).
  - For `/opt` and `/var`, you need at least 382000 KB free.

### To install and activate this version on an IPSO Diskless Appliance

1. Download `Check_Point_R70.30.ipso6_Flash.tgz` ([http://supportcenter.checkpoint.com/file\\_download?id=10738](http://supportcenter.checkpoint.com/file_download?id=10738)) for IPSO Flash-based platforms
2. Using the command shell, download the R70.30 package via ftp to `/var/tmp` on the IP Appliance.



**Note** - The installation package must be located in the `/var/tmp` directory.

3. Navigate to the `/var/tmp` directory.
4. Extract the tgz package by running:
 

```
tar -zxvf <file name>
```
5. Delete the tgz package by running:
 

```
rm -rf <file name>
```
6. Run
 

```
./UnixInstallScript.
```
7. Reboot the appliance.
8. Follow the instructions on the screen to install the appropriate components. When prompted, stop all Check Point processes.  
Only those components required for a specific target (management or gateway) are installed automatically. When the installation finishes, each successfully installed component appears in a list followed by the word **'Succeeded'**.
9. When prompted, reboot the computer by pressing `y`.

## Installation using SmartUpdate

You can use SmartUpdate to remotely install this version on devices using the operating systems: SecurePlatform (open server or appliance), Solaris, Linux, Windows, and IPSO (disk-based or flash-based).

### To install with SmartUpdate:

1. Install this package on the Security Management Server, using the Command Line or SecurePlatform Web User Interface.

2. Open SmartUpdate and close SmartDashboard.

3. Click **Packages > Get Data from All**.

When the `Operation Status` of the known gateways is **Done**, the installed packages and their versions are listed.

4. Open the Package Repository: **Packages > View Repository**.

5. Add the installation package file (\*.tgz) for each required gateway platform to the Package Repository (**Packages > Add**; or drag-and-drop).

Wait until the **Operation Status** of adding the package is **Done**. The packages appear in the Package Repository as .

6. Right-click the package and choose **Distribute**.

7. From the **Distribute Package** window, select the devices on which you want to install this version.

8. Click **Distribute**.

The installation package is distributed to and installed on the selected devices. The devices are rebooted automatically; except for Windows gateways, which must be rebooted manually.



**Note** - If after installing this version on a Windows platform, the gateway does not accept traffic, re-install the policy.

# Upgrading from NGX R60 - R65

To upgrade to the current version from versions NGX R60 - NGX R65, you must first upgrade your management, gateways and log servers to version R70 ([http://supportcontent.checkpoint.com/documentation\\_download?ID=8753](http://supportcontent.checkpoint.com/documentation_download?ID=8753)). Once you have completed this upgrade, then perform the upgrade from R70 to the current version ("[Upgrading from R70, R70.1 or R70.20](#)" on page [7](#)).

# Installing the Client Applications

The client applications that are used with this release are part of the Check Point SmartConsole.

## To install the SmartConsole:

1. Download `Check_Point_SmartConsole_R70.30_Windows.exe` ([http://supportcenter.checkpoint.com/file\\_download?id=10732](http://supportcenter.checkpoint.com/file_download?id=10732)).
2. Open the file to install the SmartConsole.

To get to the Eventia clients from the SmartDashboard, select **Window** and then choose either **IPS Event Analysis**, **Eventia Reporter** or **Eventia Analyzer**.

Refer to the appropriate Initial Configuration section ("[Initial Configuration](#)" on page 15) for information on configuring IPS Event Analysis, Eventia Analyzer server, Eventia Correlation Unit, and Eventia Reporter server.

## To install the Provider-1 MDG:

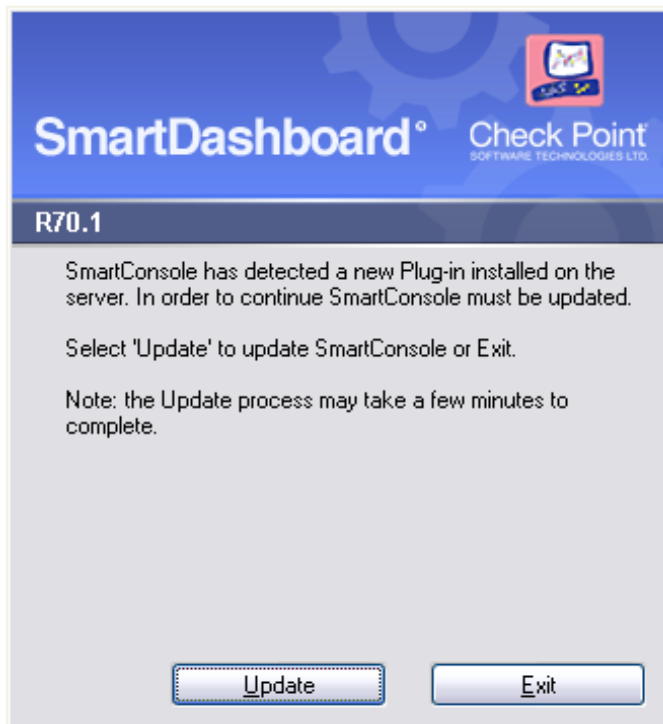
1. Download `Check_Point_Prov1Gui_R70.30_Windows.exe` ([http://supportcenter.checkpoint.com/file\\_download?id=10733](http://supportcenter.checkpoint.com/file_download?id=10733)).
2. Open the file to install the SmartConsole.

# Starting SmartDashboard for the First Time

## To launch SmartDashboard for Security Management servers:

1. Click on the SmartDashboard icon on your desktop or taskbar. Alternatively, run **Start > All Programs > Check Point SmartConsole R70.x > SmartDashboard**.
2. Enter your administrator user name and password as required.
3. Enter or select the Security Management server from the list.

If you have a SmartDashboard of a lower version than R70.30, you will get a popup message similar to the following telling you to update SmartDashboard. This is because only the R70.30 SmartDashboard can connect to the R70.30 Security Management Server.



Click **Update** to update SmartDashboard to the correct version.

## To launch the Provider-1 Global SmartDashboard:

1. In the Provider-1 MDG, click **Global Properties** in the Selection Bar.

2. In the Global Policies pane, right-click **Provider-1** and select **Launch Global SmartDashboard** from the **Options** menu.

**To launch SmartDashboard for a Provider-1 CMA:**

1. In the Provider-1 MDG, click **General** in the Selection Bar and then click the MDS Contents icon directly above.
2. Right-click **Provider-1** and select **Launch Global SmartDashboard** from the **Options** menu.

## Your First Session

If, in the **SmartWorkflow Configuration Wizard**, you chose to **use SmartWorkflow for visual change tracking**, you continue to work in SmartDashboard as usual and will not have sessions. If you chose to **use SmartWorkflow to track, review and require approval for changes**, SmartWorkflow launches for the first time with Role Segregation and sessions enabled. When you open SmartDashboard for the first time after enabling SmartWorkflow, the **Session Management** window appears together with a **New Session** window.

**To open your first session:**

1. Type a session name in the **Name** field.
2. Optionally, enter descriptive text in the **Notes** field.
3. Click **OK** to continue. SmartDashboard opens.

# Chapter 4

---

## Initial Configuration



**Note** - Read this chapter if you have upgraded to R70.30 and have not yet deployed Event correlation, IPS Event Analysis or SmartWorkflow.

Once you have installed the R70.30 package on your management servers, dedicated log servers and gateways, you must then perform initial configuration tasks for the new and updated software blades and features.

The following sections present specific procedures for performing the initial configuration. These procedures assume that you have already installed R70.30 on all relevant computers and servers.

### In This Chapter

<a href="#">Configuring Event Correlation &amp; Reporting</a>	15
<a href="#">Configuring IPS Event Analysis</a>	19
<a href="#">Configuring SmartWorkflow</a>	21

## Configuring Event Correlation & Reporting

The following sections present procedures for performing initial configuration of the Event Correlation software blade and the Reporting software blade. The specific procedures vary according to different deployment scenarios.

### Standalone Deployment

In a standalone deployment, all components of the Event Correlation and Reporting blades, together the log server functionality, are installed on a Security Management Server. Dedicated log servers are not included in this deployment.

#### To configure Event Correlation and Reporting Blade components on a standalone Security Management Server:

1. If you have an Event Correlation Blades license, install it on the Security Management server. If you do not yet have a license, you will automatically receive a 15-day trial. For more information about adding licenses, see the SmartUpdate section of the *R70.20 Security Management Server Administration Guide* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10510](http://supportcontent.checkpoint.com/documentation_download?ID=10510)).
2. Connect to the Security Management server using SmartDashboard.
3. Double-click the Security Management Server network object.
4. On the **General Properties** page, select the **Management** blade tab
5. Select to enable one or more of the following software blades the standalone Security Management Server:
  - Reporting
  - Event Correlation - Eventia Analyzer Server
  - Event Correlation - Event Correlation Unit
6. **Save** the changes.
7. Select **Policy > Install Database** to install the database on the Security Management Server.
8. On the Security Management Server CLI, run `evconfig` and follow the on-screen instructions to configure the log server to enable the following components:
  - Eventia Reporter (Reporting blade)

- Eventia Analyzer Server (Event Correlation blade)
  - Eventia Correlation Unit (Event Correlation blade)
9. Run `evstop` and then `evstart`.
  10. If you have installed the Eventia Analyzer server and/or the Eventia Correlation Unit, connect to the Security Management Server using the Eventia Analyzer client.
    - Select the **Policy** tab.
    - In the navigation tree, select **General Settings > Initial Settings > Correlation Units**.
    - Click **Add** to add those servers defined as Eventia Correlation Units.
    - In the **Correlation Unit** window, add the log servers associated with the Correlation Unit. Repeat this step for each Correlation Unit.

If Correlation Units do not appear in the list, wait until object synchronization finishes. The **Status of Object Synchronization** can be seen in the **Overview** tab.
  11. If you have installed Eventia Reporter, connect to the Security Management Server using the Eventia Reporter client.
    - In the Eventia Reporter client, click Management, located by default in the bottom left-hand corner of the screen,
    - Select **Consolidation > Sessions > Create New**.
    - In the **New Consolidation Session** window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
    - Configure and schedule reports as required.
    - Install the Event Policy by selecting **Actions > Install Event Policy**.

## Distributed Deployment

This deployment scenario uses a Security Management Server together with one or more dedicated log servers.

### Log Server Configuration

**To configure a dedicated log server computer, perform the following tasks:**

1. If you have already done so, install an Event Correlation Blade license on the log server.
2. On the dedicated log server, run `evconfig` and follow the on-screen instructions to configure the log server to enable the following components as required by your deployment:
  - Eventia Reporter (Reporting blade)
  - Eventia Analyzer (Correlation blade)
  - Event Correlation Unit (Event Correlation blade)
3. Run `evstop` and then `evstart`.

### Security Management Server Configuration

**To configure your Security Management Server:**

1. Connect to your Security Management Server using SmartDashboard,
2. Select the host network object representing the dedicated log server.
  - If you are defining a new dedicated log server, create a new host object.
3. On the **General Properties** page of the Security Management server object, select the **Management blades** tab, select the components you want to run on that computer. Enable any or all of the following Software Blades according to your deployment:
  - Reporting
  - Event Correlation - Eventia Analyzer Server
  - Event Correlation Unit
4. **Save** changes.

5. Select **Policy > Install Database** and install the database on all defined log servers.

## Eventia Analyzer & Eventia Reporter Configuration

The following steps apply to installations on new server machines. If you have previously installed these applications, you can safely skip these steps.

To configure Eventia Analyzer and Eventia Reporter do one of these procedures:

If you have installed an Eventia Analyzer server or an Event Correlation Unit, or both, on this log server, connect to the log server using the Eventia Analyzer client and do the following:

1. Select the **Policy** tab.
2. In the navigation tree, select **General Settings > Initial Settings > Correlation Units**.
3. Click **Add** to add those servers defined as Event Correlation Units.
4. In the **Correlation Unit** window, add the log servers associated with the Correlation Unit. Repeat this step for each Correlation Unit.

If Correlation Units do not appear in the list, wait until object synchronization finishes. The **Status of Object Synchronization** can be seen in the **Overview** tab.

If you have installed Eventia Reporter on this log server, connect to the log server using the Eventia Reporter client and perform the following:

1. In the Eventia Reporter client, click Management, located by default in the bottom left-hand corner of the screen,
2. Select **Consolidation > Sessions > Create New**.
3. In the **New Consolidation Session** window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
4. Configure and schedule reports as required.
5. Install the Event Policy by selecting **Actions > Install Event Policy**.

## Provider-1 Deployment

In a Provider-1 environment, the following software blades must reside on one or more dedicated Log servers, not on an MDS or MLM. In this instance, the dedicated Log servers do not host log files, as these files remain on the MLM.

- Reporting
- Event Correlation - Eventia Analyzer server
- Event Correlation Unit

## Log Server Configuration

**To configure a dedicated log server computer, perform the following tasks:**

1. If you have already done so, install an Event Correlation Blade license on the log server.
2. On the dedicated log server, run `evconfig` and follow the on-screen instructions to configure the log server to enable the following components as required by your deployment:
  - Eventia Reporter (Reporting blade)
  - Eventia Analyzer (Correlation blade)
  - Event Correlation Unit (Event Correlation blade)
3. Run `evstop` and then `evstart`.

## Defining Log Servers as Global Servers

**To define a log server as a Provider-1 global object:**

1. Connect to the MDS using the global SmartDashboard:
2. Define the dedicated log server as Global object.
3. In the **General Properties** page of the Security Management server Global object, in the **Management** tab, select the components you want to run on that server.

4. Establish SIC trust with the MDS.
5. Save and **Install Global Policy** on all relevant CMAs.
6. If you installed the Event Correlation Unit on one or more separate Log servers, perform the following steps:
  - Create or open host network object for each log server hosting an Event Correlation Unit.
  - On the **General Properties** page for each, select the **Event Correlation Unit** blade.
  - Save and assign the Global Policy to all relevant CMAs.
7. If you have installed an Eventia Analyzer server and/or an Event Correlation Unit on the log server, connect to the log server using the Eventia Analyzer client.
  - Select the **Policy** tab.
  - In the navigation tree, select **General Settings > Initial Settings > Correlation Units**.
  - Click **Add** to add those servers defined as Event Correlation Units.
  - In the **Correlation Unit** window, add the log servers associated with the Correlation Unit. Repeat this step for each Correlation Unit.

If Correlation Units do not appear in the list, wait until object synchronization finishes. The **Status of Object Synchronization** can be seen in the **Overview** tab.
8. If you have installed Eventia Reporter on this log server, connect to the log server using the Eventia Reporter client.
  - In the Eventia Reporter client, click Management, located by default in the bottom left-hand corner of the screen,
  - Select **Consolidation > Sessions > Create New**.
  - In the **New Consolidation Session** window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
  - Configure and schedule reports as required.
  - Install the Event Policy by selecting **Actions > Install Event Policy**.

## ***Defining the Reporting or Eventia Analyzer Server as a Local Server***

### **To define the server as a Local server:**

1. Connect using SmartDashboard to the CMA that manages the dedicated log server
2. Create or open a dedicated log server object.
3. On the **General Properties** page of the Security Management server object, select the **Management** blades tab, select the components you want to run on that computer. Enable any or all of the following Software Blades according to your deployment:
  - Reporting
  - Event Correlation - Eventia Analyzer Server
  - Event Correlation Unit.
4. Establish **SIC** with the CMA, and click **OK**.
5. **Save** changes.
6. Select **Policy > Install Database** and install the database on all management objects.
7. If you have installed an Eventia Analyzer server and/or an Event Correlation Unit on this log server, connect to the log server using the Eventia Analyzer client.
  - Select the **Policy** tab.
  - In the navigation tree, select **General Settings > Initial Settings > Correlation Units**.
  - Click **Add** to add those servers defined as Event Correlation Units.
  - In the **Correlation Unit** window, add the log servers associated with the Correlation Unit. Repeat this step for each Correlation Unit.

If Correlation Units do not appear in the list, wait until object synchronization finishes. The **Status of Object Synchronization** can be seen in the **Overview** tab.

8. If you have installed Eventia Reporter on this log server, connect to the log server using the Eventia Reporter client.
  - In the Eventia Reporter client, click Management, located by default in the bottom left-hand corner of the screen,
  - Select **Consolidation > Sessions > Create New**.
  - In the **New Consolidation Session** window, add consolidation sessions for all log servers. If log servers do not appear in the list, wait until the Object Synchronization process finishes.
  - Configure and schedule reports as required.
  - Install the Event Policy by selecting **Actions > Install Event Policy**.
9. Install the **Event Policy** on the Correlation Units.

## Configuring IPS Event Analysis

The following sections present procedures for performing initial configuration of the IPS Event Analysis software blade and its associated processes. The specific procedures vary according to different deployment scenarios.

### Standalone Deployment

#### To configure IPS Event Analysis to run on a Security Management Server:

1. If you have an Event Correlation Blades license, install it on the Security Management server. If you do not yet have a license, you will automatically receive a 15 day trial. For more information about adding licenses, see the SmartUpdate section of the *R70.20 Security Management Server Administration Guide* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10510](http://supportcontent.checkpoint.com/documentation_download?ID=10510)).
2. Connect to the Security Management Server using SmartDashboard.
3. Select the Security Management Server.
4. On the **General Properties** page, select the **IPS Event Analysis** blade.
5. **Save** changes.
6. Select **Policy > Install Database** and install the database on all modified objects.

### Distributed Deployment

#### To configure IPS Event Analysis server to run on a dedicated Log server:

1. If you have an IPS Event Analysis Blade license, install it on the Security Management server. If you do not yet have a license, you will automatically receive a 15 day trial license. For more information about adding licenses, see the SmartUpdate section of the *R70.20 Security Management Server Administration Guide* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10510](http://supportcontent.checkpoint.com/documentation_download?ID=10510)).
2. On the dedicated Log server, configure it as IPS Event Analysis server using the following CLI commands:
  - Run `evconfig`.
  - Press **4** and **Enter** to enable IPS Event Analysis.
  - Press **5** and **Enter** to enable IPS Event Correlator.
  - Press **6** and **Enter** to save the configuration and exit `evconfig`.
  - Run `evstop` and then `evstart`.
3. Connect with SmartDashboard to the management computer use the following steps to create a Network object for the new dedicated Log server.
  - Right-click **Network Object** in the Objects Tree and select **Host**.
  - Enter the name and IP address of the new server.
  - Establish **SIC** with the Security Management server.

- In the Software Blades **Management** tab of the dedicated Log server object's **General Properties** page, select **IPS Event Analysis**.
  - Click **OK**.
4. **Save** changes.
  5. Select **Policy > Install Database** and install the database on all management objects.

## Provider-1 Deployment

Once you have installed the release package on the Provider-1 MDS, you can then configure your Provider-1 environment to use IPS Event Analysis.

### To configure IPS Event Analysis in a Provider-1 Environment:

1. If you have an IPS Event Analysis license, install it on the Security Management server. If you do not yet have a license, you automatically receive a 15 day trial. For more information about adding licenses, see the SmartUpdate section of the *R70.20 Security Management Server Administration Guide* ([http://supportcontent.checkpoint.com/documentation\\_download?ID=10510](http://supportcontent.checkpoint.com/documentation_download?ID=10510)).
2. On the dedicated Log server, configure it as IPS Event Analysis server using the following CLI commands:
  - Run `evconfig`.
  - Press **4** and **Enter** to enable IPS Event Analysis.
  - Press **5** and **Enter** to enable IPS Event Correlator.
  - Press **6** and **Enter** to save the configuration and exit `evconfig`.
  - Run `evstop` and then `evstart`.
3. Open the Provider-1 client and connect to the MDS.
4. Enable the IPS Event Analysis Blade for all relevant CMAs in the Management Plug-ins section of the Provider-1 client.
5. Decide whether the IPS Event Analysis server will be a Global server connected to the MDS, or a local server connected to a CMA.
  - **Global server** - Open the Global SmartDashboard for the relevant Global Policy.
 

**Note** - All CMAs must be assigned to the Global Policy. To do this, right-click on the Global Policy and click **Assign Policy**.
  - **Local server** - Open the SmartDashboard for the relevant CMAs.
6. Create a Network object for the new dedicated Log server.
  - Right-click **Network Object** in the Objects Tree and select **Host**.
  - Enter the name and IP address of the new server.
  - Establish **SIC** with the Security Management server.
  - In the Software Blades **Management** tab of the dedicated Log server object's **General Properties** page, select **IPS Event Analysis**.
  - Click **OK**.
7. Click **Save**.
8. (For Local server only) Select **Policy > Install Database** and install Database on all management objects.

# Chapter 5

---

## Configuring SmartWorkflow

This section presents the procedures for the initial setup for SmartWorkflow, including the following tasks, which should be performed in sequence:

- Assigning permissions for administrators and managers in the Security Management Server and Provider-1 environments. You should define your initial users and assign permissions before enabling SmartWorkflow.
- Enabling the SmartWorkflow Blade globally for each Security Management server or CMA and choosing whether or not to utilize **sessions**.
- Starting SmartDashboard for the first time.
- Performing the initial SmartWorkflow configuration.

In This Chapter

<a href="#">Assigning Permissions</a>	21
<a href="#">Enabling the SmartWorkflow Blade</a>	22
<a href="#">Configuring SmartWorkflow Properties</a>	24

## Assigning Permissions

In a full change management scenario, with Role Segregation enabled, only managers are authorized to approve sessions, enable or disable SmartWorkflow, and configure SmartWorkflow itself. You can choose to disable Role Segregation.

When working with Provider-1, only Provider-1 and Customer Superusers are authorized to approve sessions, enable, disable, and configure SmartWorkflow.

You should always define your initial set of users and assign their permissions before enabling SmartWorkflow. This is necessary to prevent SmartWorkflow from enforcing Role Segregation before you assign manager permissions.

## Defining Permissions for Security Management Server

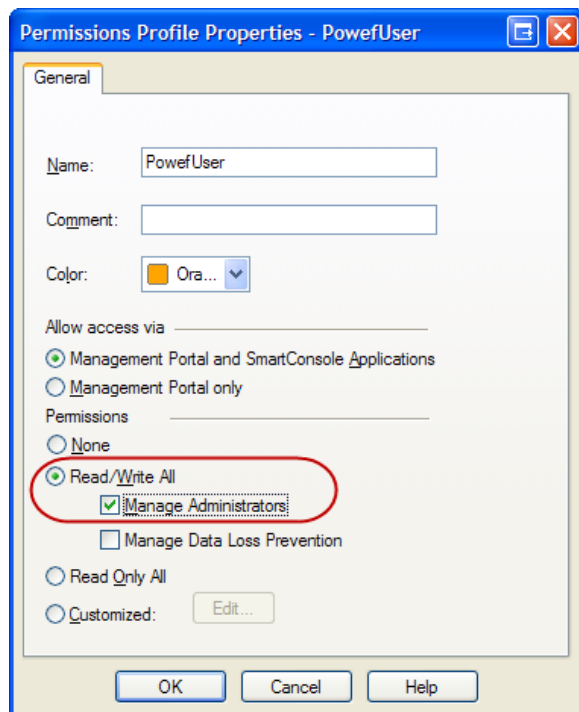
**To configure permission profiles for administrators and managers in a Security Management Server environment:**

1. In SmartDashboard, select **Manage > Permissions Profiles**.
2. Select an existing profile or click **New** to create a new profile.
3. Enter a name for the permission profile.
4. Configure the **Allow access via** parameter as required for your environment.
5. Enable **Read/Write All** for both managers and administrators.
6. For Managers only, enable the **Manage Administrators** option.



**Note** - We strongly recommend not to enable the **Manage Administrators** option for ordinary administrators, because this action allows administrators to change the SmartWorkflow configuration or to disable it entirely.

You can disable Role Segregation on the **Global Properties > SmartWorkflow** page without allowing administrators to configure or disable SmartWorkflow.



## Defining Permissions for Provider-1

To configure manager permissions for Provider-1:

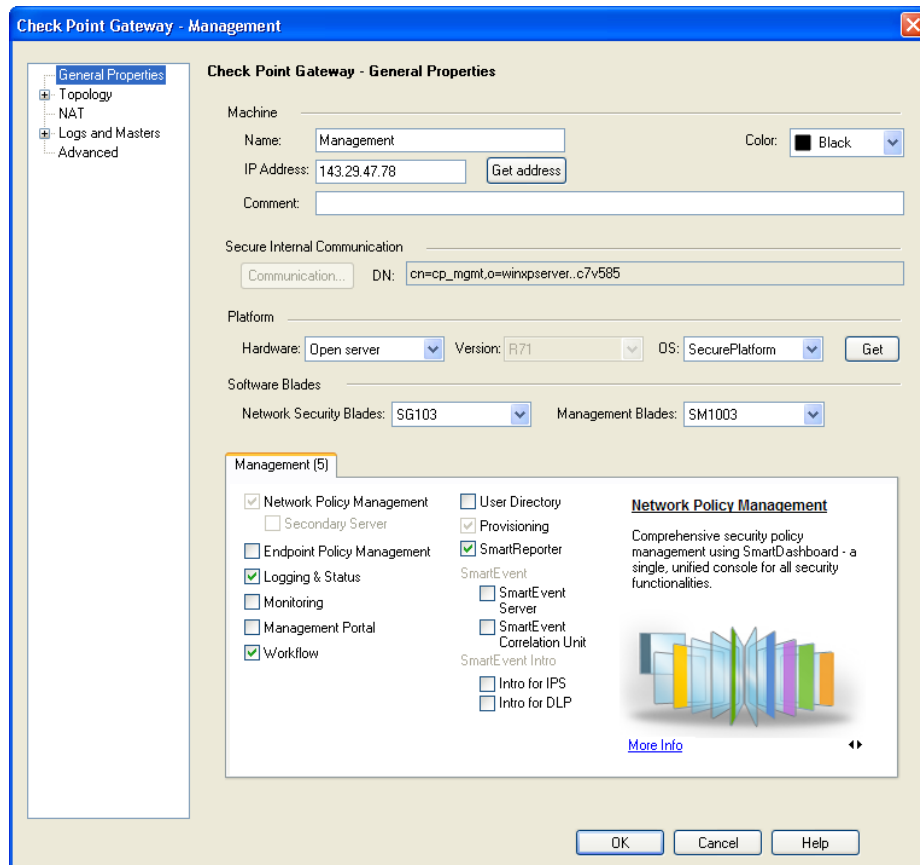
1. In the Provider-1 MDG, click **Administrators** on the **Selection Bar**.
2. In the **Customers per Administrator** pane, double-click an existing user or right-click the **Provider-1** icon and choose **New Administrator**.
3. In the **Edit Administrator** window, select either **Customer Superuser** or **Provider-1 Superuser** for managers. Select any other permission for administrators as required.
4. Define other user properties as required.

## Enabling the SmartWorkflow Blade

You must enable SmartWorkflow in SmartDashboard for each Security Management server before you can begin working with it. Once SmartWorkflow is enabled, the SmartWorkflow toolbar and menus are available when you re-open SmartDashboard.

To enable SmartWorkflow for a Security Management server:

1. In SmartDashboard, double-click an *active* Security Management server object and select **General Properties**. The Security Management server can be primary or secondary but it must have an IP address identical to the server you are connected to.



2. In the **Software Blades** section, select the **Management** tab and then select **Workflow**. The **SmartWorkflow Configuration Wizard** opens.
3. In the **SmartWorkflow Configuration Wizard** choose your mode of working with SmartWorkflow.
  - **Use SmartWorkflow for visual change tracking** allows you to track changes to the policy without sessions, so that you can install the policy without following an approval process.
  - **Use SmartWorkflow to track, review and require approval for changes** allows you to track changes to the policy with sessions, enforcing that a policy cannot be installed until it has been approved by a manager.
4. Save the configuration.

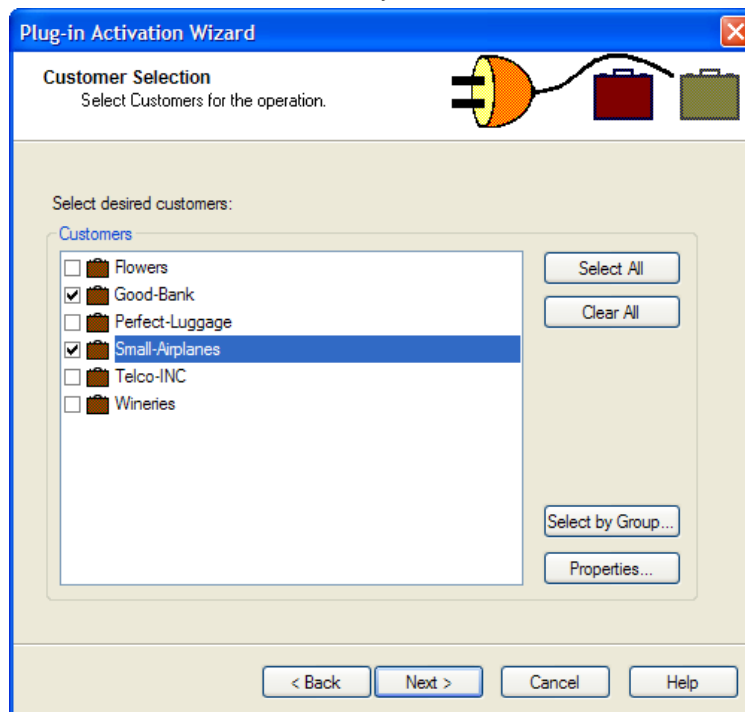
#### To disable SmartWorkflow for a Security Management server:

1. In SmartDashboard, double-click a Security Management server object and select **General Properties**.
2. In the **Software Blades** section, select the **Management** tab and clear **Workflow**.
3. Save the configuration.

#### To enable SmartWorkflow in Provider-1:

1. In the Provider-1 MDG, click **Management Plug-ins** on the **Selection Bar**.
2. Select one or more CMAs.
3. Right-click and select **Activate Plug-in on customers**.

- Select the customers for which you wish to activate the Workflow plug-in.



- In the **Plug-in Selection** window, select the **Workflow Blade**.
- Click **Finish** to install the plug-in. This may take several minutes to complete.
- In the CMA SmartDashboard, double-click the CMA object and select **General Properties**.
- In the **Software Blades** section, select the **Management** tab and then select **Workflow**.
- Save the configuration.
- When you want to work with SmartWorkflow in Global SmartDashboard, all configuration changes are made from the **Global Properties** window.

#### To disable SmartWorkflow in Provider-1:

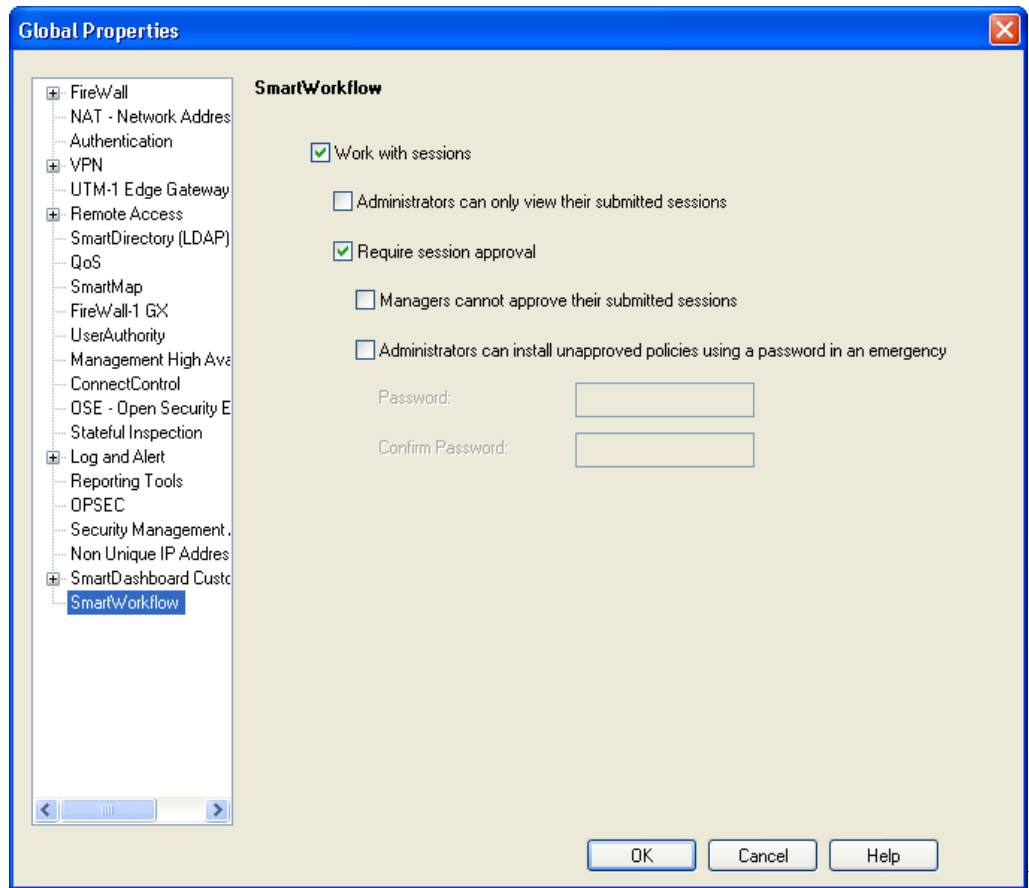
- In the CMA SmartDashboard, double-click the CMA object and select **General Properties**.
- In the **Software Blades** section, select the **Management** tab and clear the **Workflow** blade.
- Save the configuration.

## Configuring SmartWorkflow Properties

You must now configure SmartWorkflow properties in SmartDashboard. In a Provider-1 environment, you perform these configuration steps for each CMA.

#### To configure SmartWorkflow properties:

- In SmartDashboard, select **Policy > Global Properties**.
- On the **Global Properties** window, select **SmartWorkflow** from the navigation tree.



3. Sessions are enabled by default. If you choose NOT to work with sessions, clear the **Work with sessions** option. In this case, all other options are disabled.
4. Select **Administrators can only view their submitted sessions** to allow administrators to view only their own sessions. Managers can view all sessions.
5. Role Segregation is enabled by default. If you choose NOT to use Role Segregation, clear the **Require session approval** option. If you enable Role Segregation, configure the following:
  - Enable **Managers cannot approve their submitted sessions** if you do not want to allow managers to approve their own sessions.
  - Enable **Administrators can install unapproved policies using a password in an emergency** to grant administrators the ability to install a policy for an unapproved session, in emergency situations, by entering a password. The session remains unapproved after the policy installation. Enter and confirm the emergency password in the designated fields.

# Chapter 6

---

## Uninstalling R70.30



**Note** - Uninstallation from IPSO flash-based appliances is not supported. To uninstall R70.30 from IPSO flash-based appliances, you must uninstall the entire `cpsuite` package and then perform a clean install of R70.

### To uninstall R70.30:

1. Disable the R70.30 IPS Event Analysis and/or SmartWorkflow Software Blades. If you already disabled SmartWorkflow before upgrading to R70.30, you do not need to disable the SmartWorkflow Software Blade.
  - In Security Management Server deployments, deselect the Software Blades in the Security Management server's object.
  - In Provider-1 deployments, disable the active plug-ins from each CMA as follows:
    - (i) Login to the Provider-1 MDG
    - (ii) In the **Management Plug-in** tab, for each activated plug-in, right click and select **Deactivate**.
2. Run the following command on each management server and dedicated log server:
  - **All non-Windows platforms:**

```
/opt/CPUninstall/R70.30/UnixUninstallScript
```
  - **Windows platforms:**

At the command prompt, navigate to  
C:\Program files\CheckPoint\CPUninstall\R70.30  
Run  
Uninstall.bat



**Note** - After uninstalling this release from a SecurePlatform machine, the command line login prompt and the Web interface Welcome screen will still display Check Point SecurePlatform R70.30 as the installed version. This is because packages related to the SecurePlatform operating system are not uninstalled during the uninstallation process. Use the `fw ver` command to see the current version of your software.

# Index

## A

Assigning Permissions • 21

## C

Configuring Event Correlation & Reporting • 15

Configuring IPS Event Analysis • 19

Configuring SmartWorkflow • 21

Configuring SmartWorkflow Properties • 24

## D

Defining Log Servers as Global Servers • 17

Defining Permissions for Provider-1 • 22

Defining Permissions for Security Management  
Server • 21

Defining the Reporting or Eventia Analyzer  
Server as a Local Server • 18

Deployment Planning • 5

Distributed Deployment • 16, 19

## E

Enabling the SmartWorkflow Blade • 22

Event Correlation & Reporting Planning • 5

Eventia Analyzer & Eventia Reporter  
Configuration • 17

## I

Initial Configuration • 15

Installation using SmartUpdate • 11

Installation Using the Command Line • 9

Installation Using the Command Line - IPSO  
Flash-Based • 10

Installation Using the Web User Interface • 8

Installing R70.30 • 7

Installing the Client Applications • 13

Introduction • 4

IPS Event Analysis Planning • 5

## L

Log Server Configuration • 16, 17

## N

New Installation • 7

## P

Provider-1 Deployment • 17, 20

## S

Security Management Server Configuration • 16

Standalone Deployment • 15, 19

Starting SmartDashboard for the First Time • 13

## U

Uninstalling R70.30 • 26

Updating Customized INSPECT Files • 7

Upgrading from NGX R60 - R65 • 12

Upgrading from R70, R70.1 or R70.20 • 7