Check Point® Enterprise Suite
Next Generation with Application Intelligence (R55)
for IPSO 3.8
Release Notes
July 20, 2004

Introduction

Thank you for using Check Point's Next Generation with Application Intelligence (R55) for IPSO 3.8. This document contains important information not included in the documentation. Review this information before installing your products.

The latest issues of both the “What's New” document for Next Generation with Application Intelligence (R55) for IPSO 3.8 and the “Resolved Issues” document from Next Generation with Application Intelligence (R54) and (R55) can be downloaded from:

http://www.checkpoint.com/techsupport/downloads.jsp

Check Point Express

Check Point Express is a new offering in NG with Application Intelligence (R55) designed to provide superior security to businesses with up to 500 employees and multiple sites. It is the industry's most comprehensive solution designed to deliver the highest levels of access control, integrated network and application level attack protection, site-to-site and Remote Access VPN, high-availability and a single intuitive, graphical user interface.

Check Point Express includes:

- VPN-1 Express gateway for protecting the privacy of site-to-site business communications over the Internet
- VPN-1 SecuRemote for protecting remote user communications over the Internet and enables secure communication to your business
- FireWall-1 for market-leading, enterprise-class security to protect critical network resources against unauthorized access
- SmartDefense for integrated network and application level attack protection
- SmartCenter Express for centrally deploying and managing all aspects of a comprehensive security infrastructure.

IMPORTANT
Before you begin installation, read the latest available version of these release notes at:
http://www.checkpoint.com/techsupport/downloads.jsp
In This Document

**General Information**
- Introduction page 1
- Check Point Express page 1
- Supported Platforms page 2
- Build numbers page 3
- Minimum Hardware Requirements page 5
- Installing Check Point Products page 5
- Uninstalling Check Point Products page 8
- Upgrade and Backward Compatibility Notes page 8
- Security Notes page 16
- Security Enhancements page 17

**Product Information**
- FireWall-1 page 18
- SmartCenter page 28
- VPN-1 page 35
- VPN-1 Edge/Embedded page 38
- SmartUpdate page 40
- SmartView Monitor page 40
- SmartView Reporter page 42
- SmartLSM page 45
- SecureXL page 46
- ClusterXL page 47
- FloodGate-1 page 50
- UserAuthority page 51
- OPSEC page 52

**Supported Platforms**

<table>
<thead>
<tr>
<th>Product</th>
<th>IPSO 3.8</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVN Foundation and VPN-1 Pro Module</td>
<td>x</td>
<td>also supported on IP2250</td>
</tr>
<tr>
<td>SmartCenter Server</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>SecureClient Policy Server</td>
<td>x</td>
<td>also supported on IP2250</td>
</tr>
<tr>
<td>ClusterXL</td>
<td>x</td>
<td>Supported only in third party mode with VRRP or IP Clustering</td>
</tr>
<tr>
<td>FloodGate-1 (VPN-1 Pro Module)</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>UserAuthority</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Check Point Next Generation with Application Intelligence (R55) for IPSO 3.8 Release Notes. Last Update — July 20, 2004

Note - IP2250 supports SVN Foundation and VPN-1 Pro Module and the SecureClient Policy Server.

Notes to Supported Platforms Table

1) The minimum screen resolution for Check Point’s SmartConsole is 800x600. Lower resolutions are not supported. Only standard installations of the above platforms are supported.


3) SmartUpdate supports managing licenses but does not support managing products from a Nokia SmartCenter Server.

4) SmartLSM ROBO gateway is supported on IPSO 3.8.

   SmartLSM Corporate Office gateway is supported on the same platforms as SVN Foundation and the VPN-1 Pro Module.

5) SmartCenter with SmartLSM enabled is supported on the same platforms as a standard SmartCenter.

   SmartCenter and SmartLSM Corporate Office gateway can be installed on the same host.

Supported Platform’s Language Testing

Check Point's SmartCenter and Enforcement Point products are supported on all language versions of our supported operating systems but are fully-tested only on the American English versions of most operating systems. In the unlikely event that you encounter any incorrect software behavior on alternate languages, open a service request with Check Point’s Technical Support team:

http://support.checkpoint.com/kb

Build numbers

<table>
<thead>
<tr>
<th>Product</th>
<th>Command</th>
<th>Platforms</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-1 Pro</td>
<td>VPN-1 Pro: $FWDIR/bin/fw ver</td>
<td>All platforms for VPN-1 Pro, 581</td>
<td></td>
</tr>
<tr>
<td>VPN-1 Edge</td>
<td>Displayed on the default portal page</td>
<td>VPN-1 Edge can be managed from: Windows 2000, Solaris, SecurePlatform, Linux</td>
<td>VPN-1 Edge 5 R-4057</td>
</tr>
<tr>
<td>VPN-1 Pro Backward Compatibility</td>
<td>Solaris: /opt/CPfwbc-41/bin/fw ver Window: %FWDIR%\bin\fw ver</td>
<td>All platforms</td>
<td>623</td>
</tr>
</tbody>
</table>

Build numbers

<table>
<thead>
<tr>
<th>Product</th>
<th>Command</th>
<th>Platforms</th>
<th>Build Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-1 Pro</td>
<td>VPN-1 Pro: $FWDIR/bin/fw ver</td>
<td>All platforms for VPN-1 Pro, 581</td>
<td></td>
</tr>
<tr>
<td>VPN-1 Edge</td>
<td>Displayed on the default portal page</td>
<td>VPN-1 Edge can be managed from: Windows 2000, Solaris, SecurePlatform, Linux</td>
<td>VPN-1 Edge 5 R-4057</td>
</tr>
<tr>
<td>VPN-1 Pro Backward Compatibility</td>
<td>Solaris: /opt/CPfwbc-41/bin/fw ver Window: %FWDIR%\bin\fw ver</td>
<td>All platforms</td>
<td>623</td>
</tr>
<tr>
<td>Component</td>
<td>Directory</td>
<td>Platform</td>
<td>Version</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SmartConsole (GUI)</td>
<td>Help&gt;About Check Point SmartDashboard</td>
<td>Windows, Solaris</td>
<td>127</td>
</tr>
<tr>
<td>SVN Foundation</td>
<td>$CPDIR/bin/cpshared_ver</td>
<td>Windows, Solaris, Linux, IPSO</td>
<td>577</td>
</tr>
<tr>
<td>SecuRemote/SecureClient</td>
<td>Help&gt;About</td>
<td>Windows</td>
<td>082</td>
</tr>
<tr>
<td>SecurePlatform</td>
<td>ver</td>
<td>SecurePlatform</td>
<td>179</td>
</tr>
<tr>
<td>SecureClient Policy Server</td>
<td>$FWDIR/bin/dtps_ver</td>
<td>Windows, Solaris, Linux, IPSO, SecurePlatform</td>
<td>551</td>
</tr>
<tr>
<td>SmartView Monitor</td>
<td>$FWDIR/bin/rtm_ver</td>
<td>Windows, Solaris, Linux, IPSO, SecurePlatform</td>
<td>551</td>
</tr>
<tr>
<td>SmartView Reporter</td>
<td>$RTDIR/bin/SVRServer_ver</td>
<td>Windows, Solaris, Linux, IPSO, SecurePlatform</td>
<td>551</td>
</tr>
<tr>
<td>FloodGate-1</td>
<td>$FGDIR/bin/fgate_ver</td>
<td>Windows, Solaris, Linux, IPSO, SecurePlatform</td>
<td>553</td>
</tr>
<tr>
<td>FloodGate-1 Backward Compatibility</td>
<td>Solaris: /opt/CPfwbc-41/bin/fgate ver</td>
<td>Windows, Solaris</td>
<td>607</td>
</tr>
<tr>
<td>UserAuthority Server</td>
<td>$UAGDIR/bin/netsod d -v</td>
<td>Windows, Solaris, Linux, IPSO, SecurePlatform</td>
<td>552</td>
</tr>
<tr>
<td>VPN-1 HW Accelerator I</td>
<td>n/a</td>
<td>Windows, Solaris</td>
<td>5</td>
</tr>
<tr>
<td>VPN-1 HW Accelerator II</td>
<td>n/a</td>
<td>Windows, Solaris, Linux, SecurePlatform</td>
<td>12</td>
</tr>
<tr>
<td>VPN-1 HW Accelerator III</td>
<td>n/a</td>
<td>Windows, Solaris, Linux, SecurePlatform</td>
<td>15</td>
</tr>
</tbody>
</table>
**Minimum Hardware Requirements**

In This Section

| Minimum Hardware Requirements — IPSO page 5 |

**Minimum Hardware Requirements — IPSO**

TABLE 1-2 lists the minimum hardware requirements for installing IPSO

| TABLE 1-2 Minimum Requirements IPSO |
|-----------------|-----------------|
| **Platform**    | IP120, IP130, IP330, IP350, IP380, IP440, IP530, IP650, IP710, IP740, IP2250, IP1260 |
| **Memory**      | 128 Mbytes |

**Installing Check Point Products**

In This Section

<table>
<thead>
<tr>
<th>The Recommended Installation Method page 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Specific Installation Notes page 6</td>
</tr>
<tr>
<td>Upgrade Paths page 7</td>
</tr>
<tr>
<td>Minimum Screen Resolution page 7</td>
</tr>
</tbody>
</table>

**The Recommended Installation Method**

The installation methods are listed below in the recommended order:

1) The recommended method for installing products is to use the CD wrapper. For full instructions see the “Installation and Configuration” chapter in the “Check Point SmartCenter Guide”.

2) If you wish to use an on-line copy, download a specific wrapper from the Check Point Download Center web site:

   http://www.checkpoint.com/techsupport/downloads.jsp

   For full instructions see the “Installation and Configuration” chapter in the “Check Point SmartCenter Guide”.

3) Installing individual products is not the recommended installation method. If you still wish to do so, see the “Individual Installation” document on:

   http://www.checkpoint.com/support/technical/documents/docs_r55.html

   For further information, read the section “FireWall-1” on page 18.
Platform Specific Installation Notes

Nokia IPSO 3.8

Before the Nokia Installation

1) Before installing or upgrading to Next Generation with Application Intelligence (R.55) for IPSO 3.8, be sure to upgrade the IPSO operating system to IPSO 3.8 and reboot the Nokia appliance.

2) Prior to installing FireWall-1 for Next Generation with Application Intelligence (R.55) for IPSO 3.8 on a Nokia appliance, make sure no previous FireWall-1 Next Generation with Application Intelligence (R.55) for IPSO 3.8 installation exists. No warning is issued if you attempt to install Next Generation with Application Intelligence (R.55) for IPSO 3.8 on a Nokia appliance that already has Next Generation with Application Intelligence (R.55) for IPSO 3.8 installed, but it may cause some existing packages to be deleted.

3) Make sure that the Check Point VPN-1/FireWall-1 4.1 for Backward Compatibility remains non-Active, before and after Next Generation with Application Intelligence (R.55) for IPSO 3.8 wrapper installation.

4) Confirm that you have the correct static host name associated with the external IP address of the platform. From the Voyager home page, click the System Configuration link, then click the Host Address Assignment link. If localhost is the only entry, add the hostname of the gateway and the external IP address associated with it.

5) If a previous version of VPN-1/FireWall-1 NG is already installed, the wrapper package must be installed as an upgrade, giving the VPN-1/FireWall-1 NG directory as the upgrade parameter (see Command Line Installation, below). If you want to install Next Generation with Application Intelligence (R.55) for IPSO 3.8 as a new package rather than an upgrade, you must turn off any active VPN-1 Pro NG packages before you begin the installation.

6) Nokia IPSO OS images are not available on the CD. To obtain IPSO images, log into the Nokia support site on: https://support.nokia.com/.

During the Nokia Installation

7) Install the Check Point Next Generation with Application Intelligence (R.55) for IPSO 3.8 wrapper package using the newpkg command or using Voyager. This is the standard way to install all IPSO packages.

8) Installing Using the newpkg command:

You can type newpkg then press Enter and read the instructions or use the following command via the command line interface:
Clean installation

newpkg -m LOCAL -n IPSO_wrapper_R55.tgz

For NG upgrade

newpkg -m LOCAL -n IPSO_wrapper_R55.tgz -o $FWDIR

After installing via the Wrapper, the following products are installed:

<table>
<thead>
<tr>
<th>Products for</th>
<th>Status after Clean Installation</th>
<th>Status after Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>NG with Application Intelligence (R55) for IPSO 3.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check Point SVN Foundation</td>
<td>Active</td>
<td>Active</td>
</tr>
<tr>
<td>Check Point VPN-1 Pro</td>
<td>Active</td>
<td>Active</td>
</tr>
<tr>
<td>Check Point VPN-1/FireWall-1 4.1 For Backward Compatibility</td>
<td>Not Active</td>
<td>Not Active</td>
</tr>
<tr>
<td>Check Point Policy Server</td>
<td>Not Active</td>
<td>As it was prior to upgrade</td>
</tr>
<tr>
<td>Check Point FloodGate-1</td>
<td>Not Active</td>
<td>As it was prior to upgrade</td>
</tr>
<tr>
<td>Check Point UserAuthority Server</td>
<td>Not Active</td>
<td>As it was prior to upgrade</td>
</tr>
<tr>
<td>Check Point SmartView Monitor</td>
<td>Not Active</td>
<td>As it was prior to upgrade</td>
</tr>
<tr>
<td>Check Point SmartView Reporter</td>
<td>Not Active</td>
<td>As it was prior to upgrade</td>
</tr>
</tbody>
</table>

For IP2250 only the following products are installed:

<table>
<thead>
<tr>
<th>IP2250 only products for</th>
<th>Status after Clean Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NG with Application Intelligence (R55) for IPSO 3.8</td>
<td></td>
</tr>
<tr>
<td>Check Point SVN Foundation</td>
<td>Active</td>
</tr>
<tr>
<td>Check Point VPN-1 Pro</td>
<td>Active</td>
</tr>
<tr>
<td>Check Point Policy Server</td>
<td>Not Active</td>
</tr>
</tbody>
</table>

After the Nokia Installation

9) After you activate or deactivate a product using Voyager, use a terminal or console connection to login and perform `cpstop` then `cpstart`. When you activate or deactivate FloodGate-1, you must reboot the appliance.

Upgrade Paths

For additional upgrade information read Check Point’s “Upgrade Guide”. Version 4.1 SP5 or higher can be upgraded to Next Generation with Application Intelligence (R55) for IPSO 3.8. There is no need for any additional packages.

| Note - if not installing via the Wrapper, prior to installing Check Point Next Generation with Application Intelligence (R55) for IPSO 3.8 products, verify that SVN-1 Foundation Next Generation with Application Intelligence (R55) for IPSO 3.8 package is installed by running the command `$CPDIR/bin/cpshared_ver` command, and ensure the version is “NG with Application Intelligence (R55) for IPSO 3.8 - Build 577”.

Minimum Screen Resolution

It is recommended to install using a monitor with at least a minimum screen resolution of 1024x768 pixels.
Uninstalling Check Point Products

Uninstalling Individual Products

10) Uninstalling individual products documentation can be found in the "Individual Installation" document on:

http://www.checkpoint.com/support/technical/documents/docs_r55.html

This guide has both individual product installations and uninstallations.

Upgrade and Backward Compatibility Notes

For further upgrade information see “The Complete Check Point Upgrade Guide”.

In This Section

FireWall-1 page 8       SmartView Reporter page 12
SmartCenter page 9       ClusterXL page 15
Managing FireWall-1 GX page 11  FloodGate-1 page 16
VPN-1 page 11            UserAuthority page 16
SmartView Monitor page 12

FireWall-1

1) VPN-1 Pro Solaris packages have been updated with a fix to the problems related to an error message that appeared after upgrading from a version of NG prior to NG with Application Intelligence (R.55) for IPSO 3.8 stating: **FW-1: Restarting bootd**: **FW_BOOT_DIR Environment variable not defined**. To obtain a fix for existing installations and more information on this issue, refer to SecureKnowledge solution sk21234.

2) After performing an upgrade, policies with different names become different policy packages. To insert them into the same policy package, use **Copy Policy to Packages** to save the policies under the same name.

3) SAM (Suspicious Activities Monitoring) dynamic rules are not automatically upgraded from 4.1 to Next Generation with Application Intelligence.

4) Manual configuration to the file fwauthd.conf (For example: in.genericd configuration to the generic TCP Security Server) are not preserved during upgrade and the changes should be reapplied.

5) Xylan machines have not been supported since NG FP3. The same is true for Embedded Devices of the type Other. If such objects existed in the database prior to your upgrade they will appear as 4.0 Check Point objects with the same name after the upgrade.
That means that the objects will still be visible in SmartDashboard (as 4.0 Check Point Objects), but Install Policy on these Check Point objects will be blocked.

6) After upgrade from Version 4.1, in order to succeed in installing the policy, policies with 31 characters (or more) should be saved with a shorter name containing up to 25 characters.

7) If a FireWall-1 gateway object is defined in the SmartDashboard with anti-spoofing defined, and later on converted into a host gateway, compilation problems may occur when installing the policy on a Version 4.1 gateway. The workaround is to delete the object and redefine it.

8) Manually change the MAC address definitions in the local.arp Proxy-ARP configuration file if you are performing an advanced upgrade and the target machine is different than the original.

9) When trying to remove previous NG packages and NG with Application Intelligence (R55) for IPSO 3.8 is installed and active, perform the following steps:
   a. deactivate FireWall-1 (if other depended packages are active, deactivate it first)
   b. deactivate the SVN Foundation for NG with Application Intelligence (R55) for IPSO 3.8,
   c. activate the previous SVN Foundation,
   d. delete previous FireWall-1, Deactivate the previous SVN Foundation, delete the previous SVN Foundation,
   e. activate the SVN Foundation for NG with Application Intelligence (R55) for IPSO 3.8
   f. activate FireWall-1 NG with Application Intelligence (R55) for IPSO 3.8 and activate dependent products.

**SmartCenter**

1) The Upgrade process does not change the mail alert script in the Log and Alert section of the Global Properties. Check Point recommends using the `internal_sendmail` command:

   internal_sendmail [-s subject] [-t server] [-f from] email-address

2) Xylan machines have not been supported since NG FP3. The same is true for Embedded Devices of the type Other. If such objects existed in the database prior to your upgrade they will appear as 4.0 Check Point objects with the same name after the upgrade. That means that the objects will still be visible in SmartDashboard (as 4.0 Check Point objects), but Install Policy on these Check Point objects will be blocked.

3) When upgrading from 4.1 to Next Generation with Application Intelligence, cluster members that were not attached to a cluster (in Version 4.1 - they were just marked as a member) are not seen in SmartDashboard. After upgrading, these objects still exists in
the system so configuring objects with the same name is not possible. A workaround is to run the `dbedit` command to edit the `objects_5_0.C` and `objects.c` files in order to delete the hidden object.

4) When upgrading with a duplicate machine whose IP Address differ from the origin SmartCenter (Management) Server's IP Address, if central licenses are used, they should be updated to the new IP Address. This can be done via the User Center at http://usercenter.checkpoint.com, by choosing the action **License > Move IP > Activate Support and Subscription**.

5) If the AMON private schema was previously imported using the `amon_import` tool, it needs to be re-imported after the upgrade.

6) After upgrade from 4.1, policies with 31 characters (or more) should be saved with a shorter name containing up to 25 characters, in order to succeed in installing the policy.

7) Before using the command `upgrade_export` to export a configuration from a SmartCenter Server, define the environment variables `FWDIR` and `CPDIR`.

8) When upgrading from an earlier version of NG using import/export, and the new SmartCenter Server has a different IP Address than the original SmartCenter Server, a Plug-and-Play license will not be applicable on the new SmartCenter Server. The license for the SmartCenter Server should be converted to a new IP Address at http://usercenter.checkpoint.com by choosing the action **License > Move IP > Activate Support and Subscription**. The license should then be installed on the new SmartCenter Server.

9) If you are upgrading via import/export and either the import or the export operation fails for the product you are attempting to install on the machine, the entire operation will fail with the exception of these products: SmartView Reporter, SmartView Monitor, SecureXL and UserAuthority Server. Failure importing and/or exporting of these products will not fail the entire import/export operation. Use the log file of the import/export operation to understand what caused the problem and fix it. The log file is located at:
   - Windows: `C:\program files\checkpoint\CPInstLog\wrapper_R55.elg`
   - Unix: `/opt/CPInstLog/wrapper_R55.elg`

10) When upgrading a Log Server, always choose to upgrade and ignore the other options (to export the configuration or to perform pre-upgrade verifications). These options are irrelevant for Log Server upgrades. Also, the backwards compatibility (BC) package is installed on every Log Server. It can be safely removed, as it is not in use on a Log Server.
11) If downloading updates during an upgrade using the Check Point Installation Wrapper fails (for example, because the machine is not connected to the Internet), then the upgrade will continue using the tools that exist on the CD. To use the most recent version

   a. Download the updates from:
      https://support.checkpoint.com/downloads/bin/autoupdate/ut/r55/index.html
   b. Save the update on the local disk of your SmartCenter Server
   c. Restart the Wrapper and choose the second option in the Download page: I already downloaded and extracted the Upgrade Utilities.

**Managing FireWall-1 GX**

1) A direct FireWall-1 GX 1.5 management to SmartCenter R.55 is not supported. However, this upgrade can be done by using the upgrade path: FireWall-1 GX 1.5 to FireWall-1 GX 2.0.

2) When upgrading from FireWall-1 GX 2.0 a Management to VPN-1 Pro NG with Application Intelligence (R.55) for IPSO 3.8’s SmartCenter Server the FireWall-1 GX product will be deselected in in the FireWall-1 GX cluster. After upgrading the FireWall-1 GX product, recheck the FireWall-1 GX cluster object.

**VPN-1**

1) An externally managed NG FP1 VPN-1 module cannot be added to a VPN community with a star topology. When trying such configuration policy installation fails.

2) After an upgrade of a management server of a version prior to NG FP2, rules with encrypt action using AH rather than ESP (defined as part of the encrypt action properties) will fail to be transformed to ESP properly (note: starting from NG FP2, AH is not supported and upgrade process should transform such rules to use ESP instead). To make the upgrade process successful one of the following can be performed:
   • Before upgrade AH rules can be modified manually to ESP.
   • After upgrade, for upgraded encrypt rules (which were configured with AH prior to the upgrade) modify the action to accept and then back to encrypt, or disable those rules and add a new rule instead.

3) When upgrading a 4.1 Management Server to NG:
   - **before the upgrade** – rename the Internal CA back to its original name **Internal CA**
   - **after the upgrade** – reinitialization of SIC on SmartCenter is required (please note that this process requires initialization of trust between the SmartCenter Server and all the modules).
Otherwise if you modify the name of the Internal CA before the upgrade process, the Internal CA will not be functional after the upgrade.

**SmartView Monitor**

4) SmartView Monitor history reports of the SmartCenter Server are not retained in an Advance Upgrade process that imports a machine from a different Operating System. However, history reports of the remote modules are retained.

5) When downgrading Check Point VPN-1 Pro gateway, completely uninstall SmartView Monitor and all previous Real-Time Monitor installations and then reinstall the older version you desire.

**SmartView Reporter**

1) You can upgrade SmartView Reporter NG FP3 to NG with Application Intelligence (R55) for IPSO 3.8. Upgrading from NG FP2 Reporting Tool (or a prior version) is not supported. If you have an NG FP2 Reporting Tool installed, uninstall it before you upgrade to NG with Application Intelligence (R55) for IPSO 3.8.

2) When an installation of the SmartView Reporter fails on an IPSO platform an error message is not displayed on the console. Check the SmartView Reporter's installation log file to validate that the installation succeeded.

3) You must install or upgrade the SmartView Reporter via the CD. SmartUpdate does not support SmartView Reporter.

4) When performing an advanced upgrade and migrating a SmartCenter Server that contains FireWall-1 and SmartView Monitor to another machine, the Express reports for the old machine are not maintained. New reports are generated for the target machine.

5) When performing an advanced upgrade of SmartCenter with SmartView Reporter Addon, that runs on an IPSO machine, follow these steps to ensure that SmartView Reporter will function properly after your upgrade:
   a. From your SmartCenter Server perform a clean installation of Check Point suite on the IPSO machine.
   b. login to Voyager and turn to on all products that where installed in the configuration you are about to import.
   c. From a command line terminal to the IPSO machine:
      i. logout and then login to the system.
      ii. run rmdstart
d. In order to perform an advanced SmartCenter upgrade, run the upgrade_import command from the command line. For further information, see the "Upgrade Guide".

6) Report schedules are not preserved properly when performing a backout of the SmartView Reporter Server from NG with Application Intelligence (R55) for IPSO 3.8 to NG FP3. Schedules that were created or modified after the upgrade from NG FP3 should be deleted before the backout and should be regenerated after the backout to NG FP3 has completed.

7) If you are performing an advanced upgrade and you are moving the Log server from one machine to another, the Log Consolidator stops. The reason is that the Log Consolidator attempts to start reading from the last log it read. But the logs are not moved to the new machine as part of the upgrade. Therefore, when performing an advanced upgrade, if you are moving the Log server from one machine to another, reinstall the Log Consolidator policy.

8) If you are upgrading SmartView Reporter from NG FP3, it is best to produce reports only from database tables that have data that was consolidated using SmartView Reporter with NG with Application Intelligence. If you wish to create reports from tables that contain data consolidated using SmartView Reporter NG FP3, you may get inaccurate report results in some cases:

• You will get inaccurate results in all reports that count files, emails, URLs or sites.
• You will get inaccurate results for units that describe a reject reason for VPN or SecureClient connections.

If you wish to get accurate report results, you can manually run the database upgrade utility. This utility will upgrade the contents of any table in your database that you specify in the command line. Before running this utility, you must make sure the database cache size is 256MB or more.

Modify $RTDIR/Database/solid.ini, and edit CacheSize value to 268435456 bytes (256MB) or more. For further information see the “SmartView Reporter User Guide” section on Changing the SmartView Reporter Database Cache Size. If your machine adheres to the minimum hardware requirements, it should have enough free memory for this cache. If you do not have enough memory, set a smaller cache size, and run the Database Upgrade utility with the parameter -r (outlined below).

To run the database upgrade utility do the following:

a. Stop all services except the database service by running the following commands:
   i. cpstop
   ii. rmdstart
   iii. cpwd_admin stop -name LC
   iv. cpwd_admin stop -name SVR
b. Run the database upgrade utility:
   i. cd $RTDIR\bin
   
   ii. SVR_DBUpgrade [-r num_rows] [Table-name | "*"
       (see parameters below)

c. Start all check point services
   i. rmdstop (may take a while)
   ii. cpstart

The valid arguments for the upgrade utility are:

| num_rows | This is an optional parameter with default value of 150000 rows. This parameter controls the number of database rows that are updated in each SQL transaction, and it should fit into the database cache.
| Table-name | The database table you wish to upgrade. For example: SVR_DBUpgrade CONNECTIONS
| "*" | Upgrade all the tables in your database. The quotation marks around the asterisk are necessary.

9) The export mechanism of the advanced upgrade does not copy the SmartView Reporter database files and the report definition files. If you wish to perform a full export that includes all the SmartView Reporter data, follow these steps:

**Steps to perform on the original machine** (the SmartCenter machine):

a. Run the cpstop command.


c. If you are going to import the configuration to another machine, copy your database files to a location that is accessible from that machine. If you are going to import the configuration to the same machine, move your database files to a location that will not be deleted when you uninstall Check Point products (i.e not under any folder of a Check Point product)

d. Backup any company logo image file(s) that you placed under $RTDIR/bin

e. Run the CD wrapper and perform the export operation.

**If you are going to import the configuration on the same machine**

Uninstall all check point products from that machine.

**Steps to perform on the new machine**

a. Perform the Import operation on the machine you selected for that purpose.

b. Run the cpstop command.

c. Restore the database files from backup to the new machine. (Do not restore the solid.ini file)

d. Restore your company logo image file(s) to $RTDIR/bin
e. Modify `solid.ini` to point to the new location of the database files.
f. Run the `cpstart` command.

10) After you perform an advanced upgrade for a SmartView Reporter distributed configuration from FP3 to Next Generation with Application Intelligence (R55) for IPSO 3.8, if the SmartCenter machine's IP address has changed, re-establish SIC between the SmartCenter and SmartView Reporter server machines.

11) When importing a configuration into a machine that has SmartView Reporter installed, select the type of SmartView Reporter installation (either standalone or add-on) that was exported.

During the import process, in the **Setup type** dialog, select either **Local SmartView Reporter installation** or **SmartView Reporter SmartCenter Add-on** - to match the exported configuration. If the wrong SmartView Reporter setup type is selected, the imported configuration will not work properly.

**ClusterXL**

1) When upgrading third party clusters the status reported by the SmartView Status and the status reported by the utility `cphaprob` may report incorrect information. Ignore this information until the upgrade process of all cluster members is complete.

2) The 15 days evaluation license that comes with every new installation is limited to one ClusterXL Load Sharing cluster. The evaluation license does permit any number of High Availability and third party clusters.

3) When upgrading a Version 4.1 Check Point High Availability cluster, if you do not wish to change the mode of the cluster, choose Legacy High Availability mode in a new ClusterXL object (and not the default value which is New High Availability). Moving to a New High Availability configuration (recommended), requires a topological change. Read more about it in the "ClusterXL" guide under Migrating from Legacy High Availability.

4) When upgrading from Version 4.1 to NG with Application Intelligence (R55) for IPSO 3.8, cluster members that were not attached to a cluster (in Version 4.1 they were just marked as a member) are not seen in SmartDashboard. After upgrading, these objects still exists in the system so configuring objects with the same name is not possible. A workaround is to run the `dbedit` command to edit the `$FWDIR/conf/objects.C` file on the SmartCenter Server, followed by an install policy, in order to delete the hidden object.

5) When some members of a cluster have already completed their upgrade to NG with Application Intelligence (R55) for IPSO 3.8, but other are still in NG with Application Intelligence (R54), if you try to install a policy on the NG with Application Intelligence (R55) for IPSO 3.8 module, SmartDashboard reports that the policy was
installed successfully. However, the ClusterXL policy negotiation fails, leaving the cluster in an inconsistent state. The reason for the negotiation failure is that modules with different versions cannot communicate with each other.

It is not recommended to install a new policy on a cluster in the middle of the upgrade process. Exceptions to this can be found in the “Upgrade Guide”. If this step is required, run the following command on all modules first:

```
fw ctl set int fwha_conf_immediate 1
```

This work-around is not required when upgrading from any version prior to NG with Application Intelligence (R55) for IPSO 3.8.

### FloodGate-1

1) When upgrading FireWall-1 to NG with Application Intelligence, if you add FloodGate-1 as a newly installed product (one that did not exist in the prior version), run `cpconfig` after completing the upgrade/installation process.

### UserAuthority

1) When using Legacy mode on SecurePlatform, the `log_server` entry in `netso.ini` should have a reversed IP address. For example, instead of 172.16.0.1 it should be 1.0.16.172.

2) When upgrading a complex UA environment, UA Servers that are used to resolve user identity should be reconfigured under the **Network Object > UserAuthority** tab in order to create more efficient configuration.

3) When using Legacy mode a few fields in **UserAuthority Server** tab in **Network Objects** in SmartDashboard have no effect. They are used only by UserAuthority Server running in **New** mode. The fields are:
   - Automatic Configuration
   - Servers that share WebAccess authentication
   - Citrix/Microsoft Terminal Services

### SmartUpdate

1) SmartUpdate does not support NG with Application Intelligence (R55) for IPSO 3.8 remote installation.

### Security Notes

1) When configuring an SMTP Security Server to strip specific file name attachments and/or specific MIME types, it is possible that some email clients will display the files that were supposed to be stripped. For configuration details refer to SecureKnowledge solution sk14634.
2) The HTTP Security Server handles a proxied or a tunneled connection request differently than earlier FireWall-1 versions. Beginning with FireWall-1 NG FP2, such requests are not allowed if they are matched with an Accept rule. However, they are still allowed if the request is matched with an Authentication or a Resource rule. This change was done in order to harden security and prevent the CONNECT from looping to the Security Server and then to another destination. In NG FP2 FTP over HTTP proxy connections are allowed when using User Authentication even if they are not allowed explicitly by a rule in the security policy. In Next Generation with Application Intelligence (R55) for IPSO 3.8, in order to further harden security, these connections are not allowed by default unless there's an explicit rule (using a URI Resource) that allows them.

**Security Enhancements**

1) ISAKMP Vulnerability - 4 May 2004 - An ISAKMP vulnerability has been discovered that affects Check Point VPN-1 products during the negotiation of a VPN tunnel. The vulnerability may cause a buffer overflow, potentially compromising the gateway. Refer to Check Point alert site for further information:
   http://www.checkpoint.com/techsupport/alerts/ike_vpn.html

2) TCP RFC Alert - April 20, 2004 - A recently published NISCC advisory (236929/TCP) describes a potential RST attack on any operating system or software that has implemented TCP based on RFC 793 and RFC 1323. Refer to Check Point alert site for further information:
   http://www.checkpoint.com/techsupport/alerts/tcp_dos.html

3) OpenSSL Vulnerability - 26 March 2004 - Recent OpenSSL advisories reveal vulnerabilities in OpenSSL. Refer to Check Point alert site for further information:
   http://www.checkpoint.com/techsupport/alerts/openssl.html

4) FireWall-1 HTTP Security Server Vulnerability - 06 February 2004 - A vulnerability in the FireWall-1 HTTP Security Servers exists that may cause it to crash in certain circumstances. Refer to Check Point alert site for further information:
   http://www.checkpoint.com/techsupport/alerts/security_server.html

5) H.323 Vulnerability - 26 January 2004 - A recent NISCC advisory reveals vulnerabilities in H.323 equipment including GateKeepers, endpoints (phones, softphones, video cameras, etc.), and firewalls that enforce H.323 security. Refer to Check Point alert site for further information:
   http://www.checkpoint.com/techsupport/alerts/h323.html
FireWall-1 Clarifications and Limitations

FireWall-1 Clarifications

1) NG introduces a new type of object called **Group with Exclusion**. Before using an object of this type as a member of another group, or in a rule base cell that includes multiple objects, consult the SecureKnowledge solution: sk14832.

2) In Next Generation with Application Intelligence (R55) for IPSO 3.8 the **S/key** authentication method is no longer supported.

**SmartDirectory**

3) Microsoft Active Directory disabled accounts no longer pass VPN-1 & FireWall-1 Password Authentication. The SmartDirectory (LDAP) server does not enforce this user limitation directly. This is now enforced by FireWall-1 by evaluating the `userAccountControl` user attribute as referenced by FireWall-1’s Microsoft_AD profile’s `AccountDisabled` attribute. Other External Authentication methods, such as SecureID, do not enforce this user limitation and this should be enforced on authentication server being used.

**General**

4) When the SmartDefense TCP Sequence Verifier feature is enabled and SecureXL is **on** or Flows acceleration is **enabled**, a message appears when you install a policy from SmartDashboard and the Sequence Verifier feature is **not** enforced.
   - For SecureXL the message displayed is **“Warning: This gateway supports SecureXL traffic acceleration. TCP Sequence Verifier (SmartDefense) will not be enforced on accelerated connections. To allow Sequence Verification, turn off acceleration on the gateway by running cpconfig”**.
   - For Flows acceleration the message is **“Flows: TCP Sequence Verifier acceleration is not supported on the gateway”**.

   To configure the TCP Sequence Verifier select the **SmartDefense Tab > Network Security > TCP** and deselect **Sequence Verifier**.

5) also in SmartCenter Status of IP51 modules is not displayed in SmartView Status.

6) As is the case with other platforms, a VPN-1 Pro module, can now have a dynamic IP address, as well as a fixed IP address on NG with application Intelligence (R55) for IPSO 3.8. For more information about Dynamically assigned IP address modules, see Check Point’s “**VPN-1**” Guide.

7) VRRP traffic between cluster member is being dropped because the source IP used for this traffic is the VRRP multicast address and not the members' own IP addresses. The workaround is to add a rule for manually accepting VRRP traffic.
8) The rule number of accounting logs for Security Server connections from Version 4.1 modules appear with \( -2 \) as the rule number in the log record instead of the actual rule numbers that were matched.

9) When working with Flows, TFTP control connections are being closed even though a data connection exists. This can happen with very long file transfers (longer than the TFTP timeout). As a result the data connection closes as well.

10) When (the “F” is supposed to be capitalized here) Flows are enabled full sanity checks are performed for Flowed (accelerated) connections for the IP layer. No sanity checks are performed on the UDP or TCP layer of flowed packets. The workaround is to disable Flows.

**Load Sharing**

11) SecurID authentication: Each cluster member should be defined separately on the ACE/Server with its unique (internal) IP. Then edit the following line to `table.def` which will send the SecurID packets with their unique IP (and not the shared IP):

```
no_hide_services_ports = { ..., <5500, 17> };.
```

**NAT**

12) Automatic ARP is not supported with IP Pool NAT.

13) When using the SmartCenter behind NAT feature, the Enforcement Module automatically chooses the SmartCenter's address and simultaneously applies NAT considerations while making this choice. There may be specific scenarios where the Enforcement module decides to contact the SmartCenter server with an address that does not suite the module's deployment. These situations include:

- Modules from versions prior to NG with Application Intelligence that are using SmartCenter behind hide NAT or when
- The NG with Application Intelligence's automatic decision does not conform with the routing of the module's deployment.

The following procedure should be performed:

a. Manually define the masters and loggers by specifying **Use local definitions for Log Servers** and **Use local definitions for Masters** and

b. by specifying the correct IP addresses on the Enforcement Module. Note the this solution has two sub-cases:
   i. The module addresses the NATed IP address when you need for it to address the real IP address.
   ii. The module addresses the real IP address and you need it to address the NATed IP address. If this is the case, in addition, specify the SIC name of the SmartCenter Server in the masters file.
14) If you are installing a SmartCenter behind NAT without a module in the following configuration:
   • a SmartCenter Management with a perimeter module defend it and
   • a remote module

If you check **Apply for VPN-1 & FireWall-1 control connections**, the remote module still addresses the real SmartCenter IP address instead of the NAT IP address. This is because by default, the SmartCenter interface does not have a topology defined.

The workaround is to:
   a. Define the Management Server as Firewall-1.
   b. Define its interface as internal with the correct topology.
   c. Uncheck the Firewall-1 definition.
   d. Install the policy on the remote module and restart.

15) Microsoft Exchange Outlook Client UDP new mail notification does not work with Hide NAT on the client. For the new mail notification both the Client and the Server need to be in both the source and the destination cells:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Server</td>
<td>MSExchange</td>
<td>Accept</td>
</tr>
<tr>
<td>Server</td>
<td>Client</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the FWDIR/libexchange.def file, enable this notification by setting

#define ALLOW_EXCHANGE_NOTIFY (as stated in the file comments).

16) Peer-to-peer H.323 connections are not supported with NAT Hide.

17) OSE objects cannot be used in NAT rules. The workaround is to define regular node objects with the same addresses and to use them instead.

**Authentication**

18) When performing manual client authentication (using port 900) to a cluster where the members' IP addresses are not routable, the URLs returned in the HTML from the replying cluster member contain the member's own non-routable IP address instead of the cluster IP address. This fails subsequent operations. The workaround is to configure the cluster to use a domain name instead of an IP address in the client authentication HTML pages, using the ahttpclientd_redirected_url global property. Make sure that your DNS servers resolves this domain name to the cluster's IP.

19) ftp with User Authentication is not supported when used with Web browsers or NAT.
20) When configuring a non-standard port for Client authentication (i.e. ports other than 900 and 259) an explicit rule in the security policy is needed to allow traffic to the FireWall-1 module on the requested port.

21) When changing the sdconf.rec file on a FireWall-1 (needed for SecurID authentication) the new ACE setting is not applied. The new ACE setting is applied after restarting the FireWall-1 services by running cpstop and cpstart.

22) Client Authentication will fail if FireWall-1 machine name is configured with a wrong IP address in the hosts file.

23) SmartDirectory search requests no longer include an empty attribute in the query attribute list. Now none of the attributes in the attribute list are empty. Empty attributes caused certain SmartDirectory servers to fail attempts at decoding the SmartDirectory search request.

24) When using SmartDirectory server for internal password authentication, if the account lockout feature is disabled the Firewall will not attempt to modify the user's login failed count and last login failed attributes on the SmartDirectory server. This will improve overall performance and will eliminate unnecessary SmartDirectory modify errors when using SmartDirectory servers that do not have these attributes defined because they did not apply the Check Point SmartDirectory schema extension on the SmartDirectory server.

25) Definition of nested RADIUS Server groups is not supported.

26) When using automatic or partially automatic client authentication for HTTP on CPLS clusters (both ClusterXL and OPSEC clusters), define a decision function based only on IP addresses in order for connections to open.

From the ClusterXL Gateway Property >Load Sharing >Advanced >select IPs (the third radio button).

Defining a decision function on OPSEC clusters products is done via the individual product. Refer to the individual product's documentation for more information.

**Security Servers**

27) The HTTP Security Server handles a proxy or a tunneled connection request differently than earlier FireWall-1 versions. Beginning with FireWall-1 NG FP2, such requests are not allowed if they are matched with an Accept rule. However, they are still allowed if the request is matched with an Authentication or a Resource rule. This change was done in order to harden security and prevent the CONNECT from looping to the Security Server and then to another destination.
In NG FP2 FTP over HTTP proxy connections are allowed when using User Authentication even if they are not allowed explicitly by a rule in the security policy. In Next Generation with Application Intelligence (R55) for IPSO 3.8, in order to further harden security, these connections are not allowed by default unless there's an explicit rule (using a URI Resource) that allows them.

28) When attempting to perform RADIUS authentication, and the RADIUS server is down, the HTTP Security Server process may fail and restart.

29) Some email clients process and display invalid attachments that use badly placed slash '/\ characters (for example 'app/lication/x-msdownload' will be processed as the correct 'application/x-mmsdownload' type). When the SMTP Security Server is configured to strip by MIME types, invalid types (like above) are not stripped, but it may appear like the correct type is being stripped.

30) When using SMTP resources to filter files by their filename, an incorrect log message is generated stating: **Forbidden MIME attachment stripped**.

31) UFP counters available via `cpstat fw -f ufp` give incorrect values.

32) If web browsers are configured to use an IP address for their proxy (instead of a hostname), the next proxy definition of the HTTP Security Server must also use the same IP address. If the next proxy definition is a hostname, connections using an IP address will not be allowed to the proxy. It is recommend to use only hostnames in the browser configuration.

33) Outlook Web Access is not supported with User Authentication.

34) When a field in a URI specification file is too long, the security server exits when trying to load the file. Under load, the FireWall-1 daemon (FWD) reloads the security server, which then exits. After a certain time cores are dumped.

35) Client authentication with **agent automatic sign on** is supported with all rules with two exceptions:
   - The rule must not use HTTP resource.
   - Rules that have hosts that were defined as web servers as destination.

36) When using SOAP filtering in the HTTP Security Server, The SOAP scheme file supports all forms of namespace and method names, however, the feature is not supported if the method has no namespace at all.

37) When FireWall-1 Security Servers are used to protect servers running on the same machine, the client-side connection and the server-side connection must use the same destination port.

38) Security Servers are not supported with Sequence Verifier in Load Sharing Cluster environments.
Anti Spoofing

39) On ClusterXL clusters, spoofed packets with the source IP of the cluster members themselves, or of the cluster IPs may be dropped by the ClusterXL module and no log will be sent telling you about it.

40) When a VPN-1 Pro Module first comes up, before the Security Policy defined by the administrator becomes active, the Default Filter is installed on the Module. Installation of the Default Filter causes anti-spoofing warnings to appear on the console (or Event Viewer on Windows NT). These messages can be ignored.

Services

41) No warning is generated when a policy containing services with the Keep connections open after Policy has been installed checked is installed on pre-Next Generation with Application Intelligence (R.55) for IPSO 3.8 modules. Such services will be enforced according to the default behavior on these modules.

42) In NG FP3 if the DCERPC service is configured with the protocol type set to MSexchange, the inspect code that enforced the MSExchange inspection replaces the regular DCERPC inspection, and therefore reduces the enforcement level of the DCERPC service. The reduced inspection means that Blaster is not blocked.

The MSExchange protocol type is needed only to allow UDP email notifications, it is still possible to use Exchange traffic without it.

It is therefore recommended not to use the MSExchange service in NG FP3. The problem does not exist in NG with Application Intelligence (R.54) and above. For further information read SecureKnowledge solution sk23070.

43) DCE-RPC services cannot be used in a rule that contains any other services or enforced in a rule with any service. The workaround is to create dedicated rules for DCE-RPC services.

44) When a SOAP request is approved, it is logged only if both Track SOAP connections is set to Log, and the matched rule Track field is also set to Log.

45) When a SOAP request is rejected because it does not match the SOAP scheme defined in the resource, a reject log is generated only if the Exception track in the General Properties of the URI resource object is set to Log. If Log is specified the matched rule Track field and additional Accept log will be generated, although the connection is actually rejected.

46) When CIFS resources are used in rules with policy targets in their Install On fields, policy installation on pre-Next Generation with Application Intelligence (R.55) for IPSO 3.8 modules may succeed without warning, although CIFS resource filtering is not supported on these modules.
47) When using MSExchange DCE-RPC services and logging there are no new logs for each Send/Receive operation performed by the client. The reason is that MSExchange clients open TCP data connections only when the session starts, these connections are kept established throughout the session's lifetime (this is different than other email systems). Each Send/Receive operation is done on the same connection and therefore it is not logged. Outlook clients are configured to automatically check for new mail every 10 minutes by default, so the data connections are kept alive in the FireWall-1 connection table even if the client is idle for a long time.

48) A service using the FTP_BASIC protocol type cannot be used with the FTP Security Server.

49) Despite the fact that the correct security policy is enforced, due to a log display issue, logs for HTTPS connections may appear as SSL_V3 connections even if you used SSL version 2.

50) When using T.120 connections, make sure you manually add a rule that allows T.120 connections.

**Web Security**

51) Web servers security is normally enabled for all node objects, however, for cluster members acting as web servers this feature is disabled. The feature will be enabled in future versions.

**Backward Compatibility**

52) Installing a combined FireWall-1 and FloodGate-1 policy on a version 4.1 VPN-1/FireWall-1 Module may fail. To resolve this, install the FireWall-1 and FloodGate-1 policies separately.

53) When managing version 4.1 Modules, changes to the connection table size are not updated on the 4.1 Modules. To update the size of the connection table, follow the instructions in SecureKnowledge solution 3.0.698764.2304823. Note that the relevant table.def file is not the one in $FWDIR/lib. It is located in the directory `/opt/CPfwbc-41/lib` for Unix platforms and `%FWDIR%\FWL_4.1_BC\lib` for Windows platforms.

54) Warning messages are displayed when installing a policy if Backward Compatibility is installed and the policy contains DAIP modules. These messages can be safely ignored.

55) When several services use the same port, it is possible to mark which one of the services should be matched for Any. If several services use the same port and all match, no warning message is generated when the policy is installed on a version 4.1 Module. For NG Modules, a warning message is generated.
56) In pre-NG with Application Intelligence modules, the parameter `http_max_request_url_length` as set by the SmartDefense Dashboard, drops all connections when it is set to 0, unlike the NG with Application Intelligence behavior which is to turn the feature off.

**IPv6**

57) In IPv6 logs, IPv6 address resolving is not supported in SmartView Tracker.

58) Discovery traffic is enabled by default on IPv6 enabled modules. To disable it, edit the file `$FWDIR/lib/implied_rules.def` and comment out the line `#define ACCEPT_DISCOVERY 1`.

59) Anti-spoofing is currently not supported with IPv6.

60) Boot policy is not supported on IPv6 enabled modules.

61) When connecting to the IPv6 IPv4 'compatible' address of FireWall-1 (::w.x.y.z., for example), the following appear on the console:

```
```

This message can be safely ignored in such configurations. In order to disable it completely, run this command:

```
modzap _fw_verbose_unknown_if $FWDIR/boot/modules/fwmod.o 0x0 and reboot.
```

62) Content of IPv6 in IPv4 tunnels (IPv4 protocol 41) passing through FireWall-1 is not inspected.

63) CPMAD functionality is not supported with the IPv6 protocol.

64) IPv6: SmartDefense's `ping size` property is not enforced on ICMPv6 echo request packets.

65) Due to the fact there is no ipv6 support for security servers, enabling **Configuration apply to all connections** under SmartDefense Applet's FTP Security Server settings causes FTP connections over IPv6 to be rejected, without any log. The same applies to HTTP and SMTP connections.

66) The command `fw6 unload localhost` unloads both IPv6 and IPv4 policies, although it should unload only the IPv6 policy.

67) IPv6 packets with extension headers which are not explicitly allowed via editing of the `table.def` INSPECT script are dropped without being logged.

68) The RSH protocol is not supported for IPv6.

**SmartConsole & SmartConsole Applications**

69) The SmartConsole Client supported for NG with Application Intelligence (R55) for IPSO 3.8 is from NG with Application Intelligence (R55).
70) FireWall-1 implied rules for SmartConsole Clients are not matched when using wildcard (e.g. 1.1.1.*) or domain name formats in the `cpconfig` SmartConsole clients definitions (e.g. support.acme.com). As a result connections from SmartConsole Clients to the SmartCenter Server may be blocked if there is a FireWall-1 module between them. Single IP definitions (e.g. 1.1.1.1) are supported. When specifying SmartConsole Clients using any formats other than the IP address, add an explicit rule in the Rule Base allowing the SmartConsole Clients to connect to the SmartCenter Server.

71) When upgrading from NG FP1 or lower, certain policies may be hidden in SmartDashboard. Starting from NG FP2, only policies that belong to the current Policy Package are displayed. To access other policies select File > Open and choose the relevant Policy Package.

72) When using Smart Directory (LDAP) to manage users on Microsoft's Active Directory, if a branch other than `cn=users` has a group that exceeds 1000 members the group's members do not show and the group appears to be empty.

**Logging**

73) When working with a Log Server of an earlier version than the version of SmartCenter Server, the logs fields of log records from new modules that were added after the upgrade of SmartCenter Server might not be resolvable.

74) FTP data connections may appear in the Active connections view in SmartView Tracker even after these connections have been terminated.

**Policy Installation**

75) There is a problem with install policy after the module policy has been explicitly uninstalled as in the following scenario:

1. There is a FireWall Module installed on the SmartCenter Server.

2. There is no policy loaded on the SmartCenter Server, either after a clean installation or when the policy was previously unloaded using the SmartConsole or a command line (`fwm unload` or `fw unloadlocal` commands).

3. The policy is being installed on both the remote Module and the SmartCenter Server at the same time.

As a workaround, install the policy separately on the SmartCenter Server and on the remote Module.

76) When installing a policy on a module Anti spoofing warning messages for other modules that are not being installed can appear in the policy installation log, if Anti spoofing is not configured on these modules.

77) Policy installation may fail when there are 70 or more dynamic objects.
OSE

78) For Cisco and 3Com routers make sure that the host names are resolvable by DNS or by the hosts file.

SAM

79) A Suspicious Activity Monitor (SAM) rule will fail for a remote gateway if the SmartCenter Server is also a FireWall-1 module and no policy has been installed on it since adding the remote gateway.

Dynamically Assigned IP Address (DAIP) Modules

80) When deleting and redefining the DAIP object in the SmartDashboard, restart the DAIP Module (perform cpstop, cpstart).

81) The \texttt{fw \ tab \ <remote \ DAIP \ Module>} command on a SmartCenter Server is not supported.

Miscellaneous

82) A Network object with \texttt{0.0.0.0} both in the address and the mask is not supported.

83) Token ring adapters are not supported.

84) The \textbf{Accept VPN-1 & FireWall-1 control connections} Implied Rules setting is applicable to a SmartCenter server object in specific cases only:
\begin{itemize}
  \item to the primary IP defined for this object and
  \item only if there are interfaces defined in its Topology tab.
\end{itemize}

This may create connectivity problems when trying to install policies (or other operations included in the control connections). The workaround is to define explicit rules that allow connectivity to the SmartCenter object.

85) When executing the following command:
\begin{verbatim}
fw tab -u -f -t connections
\end{verbatim}
The error messages can be safely ignored like \textbf{FW-1: fwkbuf_length: invalid id number XXXX} and \textbf{Table kbufs - Invalid handle 6a6b8803 (bad entry)}. In order to avoid the messages altogether, use the command:
\begin{verbatim}
fw tab -u -t connections
\end{verbatim}

Security

86) A recently published NISCC advisory (236929/TCP <http://www.uniras.gov.uk/vuls/2004/236929/index.htm>) describes a potential RST attack that may result in premature session termination. This only affects long-life TCP connections, because the attacker will need to guess all of the following:
\begin{itemize}
  \item both the IP addresses,
  \item the source and destination port, and
  \item an approximate sequence number.
\end{itemize}
FireWall-1 offers two protection solutions for this vulnerability. The first solution is based on enhanced sequence verification. The second solution detects RST floods which are typical to these kinds of attacks. For more information, see SK26137.

**SmartCenter**

**SmartCenter Clarifications and Limitations**

**Installation**

1) SmartConsole NG with Application Intelligence fails to install on machines with a 3.0 GUI installed on the same machine.

**Policy Installation**

2) After aborting an installation, before attempting to install a policy, make sure that there are no processes running the `fwm load` command on SmartCenter Server or your installation may hang.

3) Policy installation may fail when there are 70 or more dynamic objects.

**Configuration**

4) When the FireWall-1 services on one or more cluster members are stopped using the command `fwstop`, policy installation on the cluster will cause the installed policy to be inconsistent between the active and stopped members. To make sure that the installed policy is always consistent across all members use the `cpstop` command instead of the `fwstop` command.

5) SmartView Reporter supports SmartCenter High Availability with some limitations:
   - SmartView Reporter Server should be installed on a machine separate from the High Availability SmartCenter machines.
   - SIC is established between SmartView Reporter Server and the active SmartCenter machine.
   - All modules send their logs to a Log Server. The Log Server can be either one of the SmartCenter machines, or a separate machine.

After performing change over:
   - Log consolidator will continue working and processing log files from the Log Server machine.
   - You need to reestablish the SIC between the SmartView Reporter Server machine and the new active SmartCenter.
   - After re-establishing SIC, SmartView Reporter Server will resume its work, and SmartView Reporter client can connect to the new active SmartCenter.
**SmartCenter Server**

6) Embedded Devices devices of version 4.1 are unable to fetch a policy from a SmartCenter Server.

7) An NG with Application Intelligence (R55) for IPSO 3.8 SmartCenter Server can also control NG with Application Intelligence (R55) gateways. An NG with Application Intelligence (R55) SmartCenter Server can control NG with Application Intelligence (R55) for IPSO 3.8 gateways.

**SmartConsole Applications**

8) The SmartConsole Client applications from version NG with Application Intelligence (R55) are supported for this release of IPSO 3.8.

9) In order to be able to track Session ID information, an application should be opened independently, meaning not from another Check Point application.

10) When deleting objects from SmartDashboard, in some cases the **Where Used...** option will not report that objects are being used in the database, and it is possible to delete these objects without any warning. The following are cases in reference:
   a. RADIUS and TACACS servers referenced by Templates in the Authentication tab.
   b. Users and User Groups contained by other User Groups.
   c. For SmartDirectory Account Units referenced by External Groups the **Where Used...** option is applicable but the Delete operation cannot be performed. As a workaround, restart (cpstop, cpstart) the SmartCenter Server. Note that all cases apply only if the objects were created after the SmartCenter Server was started.

11) The **View rule in SmartDashboard** feature in SmartView Tracker does not bring into focus the SmartDashboard application if it is already opened to the right rule database.

12) When logs cannot be generated from some reason, such as there is no disk space or the logging process is down, then changes cannot be saved from SmartDashboard. If this occurs, the following error message appears: "**The changes could not be saves. Please make sure all Firewall-1 services are up and running. For more information use the SmartView Status application**".

13) When running a query on a Security Policy in SmartDashboard, only user-defined rules are displayed in the query result. Implied rules matching the query will not be displayed, even if the option **View Implied Rules** is selected.

14) When switching the active file from SmartView Tracker, the new active file name will be given automatically by the system, and will not get the user defined file name.

15) When choosing to view Installed Policies from SmartDashboard on Motif, you may get stuck if one of the VPN-1 Pro modules does not respond.

16) The capability for exporting logs from SmartView Tracker running on Motif is disabled in this version.
17) When upgrading from NG FP1 or lower, certain policies may be hidden in SmartDashboard. Starting from NG FP2, only policies that belong to the current Policy Package are displayed. To access other policies select File > Open and choose the relevant Policy Package.

18) When using Smart Directory (LDAP) to manage users on Microsoft's Active Directory, if a branch other than cn=users has a group that exceeds 1000 members the group's members do not show and the group appears to be empty. However SmartCenter will not crash.

19) FireWall-1 implied rules for SmartConsole Clients are not matched when using wildcard (e.g. 1.1.*.*) or domain name formats in the cpconfig SmartConsole clients definitions (e.g. support.acme.com). As a result connections from SmartConsole Clients to the SmartCenter Server may be blocked if there is a FireWall-1 module between them. Single IP definitions (e.g. 1.1.1.1) are supported. When specifying SmartConsole Clients using any formats other than the IP address, add an explicit rule in the Rule Base allowing the SmartConsole Clients to connect to the SmartCenter Server.

20) When manually defining branches on an Account Unit, spaces between elements in the branch definition will not work. Example:

A good branch: ou=Finance,o=ABC,c=us

A bad branch: ou=Finance, o=ABC, c=us

21) When a SmartDirectory user is based on an internal firewall template, internal groups that the template belongs to will be added to the SmartDirectory user, but these groups will not appear in the list of template groups in the user's Groups page.

Logging

22) Administrator with Read Only permission for Monitoring can still create, modify, rename and delete queries in SmartView Tracker.

23) If your SmartCenter Server or your Log Server are running IP2250 – Nokia's Diskless appliance, the logging policy that being defined on their objects (The 'Logs and Masters' on the object properties) will be ignored, and will be managed automatically.

24) If you define or delete an object after logging in to SmartView Tracker, it will not be shown in the Remote Files Management option of SmartView Tracker. Close and reopen the SmartView Tracker to get an update.

25) When a Log Server is installed on a DAIP module, management operations such as "purge" and "log switch" cannot be performed.

26) Audit logs operation strings have changed (starting from NG with Application Intelligence). Several new columns have been added and other existing column names have been changed. These changes might cause existing filters to stop working.
27) When working with a Log Server of an earlier version than the version of SmartCenter Server, the logs fields of log records from new modules that were added after the upgrade of SmartCenter Server might not be resolvable.

28) Configuration including a VPN-1 Edge/Embedded object and Log Server. On the Log Server, the VPN-1 Embedded Connector tries to login to fwm and fails. Subsequent to each try, two audit log records are issued: one for login and one for logout. Do as follows on your Log Server:

   a Run cpstop.

   On Windows platforms:

   b Use REGEDIT to delete the following registry key:

   \HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\SSC

   c On Unix platforms:

   d Run cp_regedit -d \SOFTWARE\CheckPoint\SSC

   e Run cpstart.

Monitoring

29) As of NG FP2, the cpstat_monitor command line utility can no longer be used to define system alert parameters. System alert parameters are now configured in the Check Point SmartView Status (see the Check Point SmartCenter Guide). The Check Point SmartCenter Server has a system alert monitoring mechanism that takes the system alert parameters you defined in SmartView Status and checks if that system alert parameter has been reached. If so, it activates the action defined to be taken.

30) Issuing a Stop Member command in SmartView Status performs the cphastop command on this member. This command also disables the State Synchronization mechanism. Any connections opened while the member is stopped will not survive a failover event, even if the member is restarted using cphastart. However, connections opened after the member is restarted are normally synchronized.

31) When defining system alerts in SmartView Status, if you choose one of the User Defined options as the Alert Method, make sure that this method is defined in SmartDashboard's Global Properties. If the alert method is not defined, a regular alert is generated.

32) When you create a new module in SmartDashboard, the module will appear with the status waiting in SmartView Status until SmartView Status is restarted. For further information refer to SecureKnowledge solution sk16122.

33) Alerts that are defined in the Check Point SmartView Status System Alert tab are not sent to the SmartView Status System Status tab as popup alerts, until a first policy is installed. In the SmartDashboard Global Properties, Log and Alert > Alert Commands page, be sure to check the property Send popup alert to SmartView Status.
34) SmartView Status should be opened connecting to a SmartCenter Server and not to a Log Server. When using SmartView Status on a Log Server, statuses may be inaccurate.

35) OS information will not be available both in SmartView Status and in SmartView Monitor if the monitored machine is a Windows machine that does not run the Windows Management Instrumentation service.

Management High Availability

36) If your primary SmartCenter Server is a Stand Alone configuration, and one of your secondaries SmartCenter Servers is active, then right after upgrade, policy installation from the secondary to the primary will be prohibited. In order to resolve this, locally install policy on the primary server.

37) When creating a Management High Availability environment, all peers must be installed with the same products. If one product is installed on one peer but not on the other, product information may be lost and the product may not function properly.

38) Management High Availability does not automatically synchronize `fw putkey shared secrets` for 4.1 VPN-1/FireWall-1 Modules. In other words, after you have established control channels between the Primary SmartCenter Server and 4.1 VPN-1/FireWall-1 Modules using `fw putkey`, you must do the same on each of the Secondary High Availability SmartCenter Servers. For example, if the High Availability configuration consists of one Primary and one Secondary SmartCenter Server and one Version 4.1 VPN-1/FireWall-1 Module, you must run `fw putkey` four times: once on the Primary SmartCenter Server, once on the Secondary SmartCenter Server, and twice on the Module (once for each SmartCenter Server).

39) A SmartCenter Server that is also a FireWall-1 module must have a policy installed on it in order for other SmartCenter Servers to be able to communicate with it. This must be done after initial setup, or after resetting SIC communication on the SmartCenter Server.

40) Database versions, which were created using the Revision Control feature, should be synchronized manually in a Management High Availability environment. In order to synchronize it you should:

1. Perform `cpstop` on the standby SmartCenter Server
2. Copy all files under $FWDIR/conf/db_versions/repository/* and $FWDIR/conf/db_versions/database/* from the active management to the standby SmartCenter Server
3. Perform `cpstart` on the standby SmartCenter Server

41) When adding a new Secondary SmartCenter, the machine should be synchronized once manually before it starts synchronizing automatically.
42) Before installing a Secondary SmartCenter, make sure its clock is synchronized with the clock of the Primary SmartCenter, or the Plug-and-Play license will not be available for the Secondary SmartCenter.

Trust Establishment (SIC)

43) When defining a new DAIP module in SmartDashboard, the recommended way to establish SIC trust is to push the SIC certificate using the current dynamic IP of the module. It is also possible to establish SIC trust from the module side by pulling the SIC certificate. In this case the following procedure is required:

a. Define the object for this DAIP module in SmartDashboard, fill in the SIC activation key and initialize SIC.

b. Pull the certificate from SmartCenter Server (using the `cp_pull_cert` command on the module).

c. Install the policy on the module; at this point the installation will fail.

d. Restart SmartCenter Server services (run `cprestart` on SmartCenter Server).

e. Fetch policy from the DAIP module.

It is recommended to establish SIC with DAIP module from SmartDashboard, while configuration the current IP of the DAIP machine in order to push the SIC certificate.

However, if SIC is established from the module side (pull instead of push), then the following procedure should be taken:

a. Configure the DAIP module and establish SIC from the module

b. Define the object for this DAIP module in SmartDashboard

c. Install the policy on the module; at this point the installation will fail

d. Issue `cpstop` and `cpstart` on the SmartCenter Server

e. The DAIP module will fetch the proper policy

SmartView Status

44) Status of IP51 modules is not displayed in SmartView Status.

FloodGate-1

45) In order to manage FloodGate-1 modules from a Nokia SmartCenter, you need to perform the following steps:

a. The product FloodGate-1 needs to be enabled in Voyager on SmartCenter.

b. Telnet into the Nokia SmartCenter and perform `cpstop` and `cpstart` (or reboot). In `cpstop`, you can safely ignore the message `etmstop: Module not loaded`. When you run `cpstart` on SmartCenter, you can safely ignore the message `FloodGate-1: This is a Management Server. No QoS Policy will be Loaded`.

Trying to install a QoS policy on a module before executing these steps on SmartCenter, will fail with the error message: `Failed to start uninstall/install operation`. 
**Backward Compatibility**

46) Warning messages are displayed when installing a policy if Backward Compatibility is installed and the policy contains DAIP modules. These messages can be safely ignored.

47) When several services use the same port, it is possible to mark which one of the services should be matched for Any. If several services use the same port and all match, no warning message is generated when the policy is installed on a version 4.1 Module. For NG Modules, a warning message is generated.

48) Installing a combined FireWall-1 and FloodGate-1 policy on a version 4.1 VPN-1/FireWall-1 Module may fail. To resolve this, install the FireWall-1 and FloodGate-1 policies separately.

**OSE**

49) The Drop action is not supported for 3Com and Cisco OSE devices. If the Drop action is used, the policy installation operation fails.

50) For Cisco and 3Com routers make sure that the host names are resolvable by DNS or by the hosts file.

**Dynamically Assigned IP Address (DAIP) Modules**

51) The fw tab <remote DAIP Module> command on a SmartCenter Server is not supported.

52) When deleting and redefining the DAIP object in the SmartDashboard, restart the DAIP Module (perform cpstop, cpstart).

**Miscellaneous**

53) Using the cp_merge utility to merge large number of objects (more than 10,000) from two SmartCenter Servers may not work. This is because at some point two many audit logs are generated. If you have a large number of objects, and you wish to perform the merge even though from some point the audit logs will not be generated, then do as follows:
   a. Define the environment variable FWM_ALLOW_AUDIT_FAILURE from a shell
   b. Use the cp_merge command from the same shell

54) After upgrade from NG FP2, the name of Internal Certificate Authority (CA) that was previously entered is not displayed in Check Point Configuration Tool (cpconfig > Certificate Authority tab), although it is still viable. If it is reconfigured, then it is displayed.
VPN-1

VPN-1 Clarifications and Limitations

VPN Routing

1) When using VPN routing to route all communication from the VPN domain of a Satellite Gateway via the Hub to other Satellite Gateways or to the Internet, it is not possible to open connections from the external IP of the Satellite Gateway to the Internet.

2) The IP pool NAT on a VPN-1 module which serves as a VPN router (enables forwarding of VPN traffic from one VPN tunnel to another) should be defined as part of the encryption domain of the VPN router. Otherwise, VPN connections via the VPN router might fail.

3) VPN Routing only connects the VPN domain of a DAIP gateway that is hosted behind the DAIP gateway to the VPN domain of another DAIP Gateway. Connections that are originated on the DAIP gateway itself or directed at the DAIP gateway itself cannot be routed through the Hub.

VPN Communities

4) SmartDashboard enables adding VPN-1 modules with dynamic IP address as members of a VPN community in which aggressive mode for IKE Phase 1 is selected. This configuration is not supported.

5) Defining services in the clear in the community (available in gateway-to-gateway communities) is not supported if one of the internally managed members is of version earlier than NG FP3.

6) Disabling NAT in the community (available in gateway-to-gateway communities in the advanced properties tab) is not supported if one of the internally managed members is of version earlier than NG FP3.

7) A pre-shared secret defined for externally managed VPN modules in the community is not supported if one of the internally managed members is of version earlier than NG FP3.

8) If Exportable for SecuRemote/SecureClient is checked on a VPN-1/ FireWall-1 Enforcement Module (from the VPN tab under Traditional Mode configuration), the modules topology information will be exported to SecuRemote/SecureClients even if the Enforcement Module is not a member of the Remote Access community.
**VPN-1 Clusters**

9) Peer or secure remote gateways may show error messages when working against an overloaded gateway cluster in load-sharing mode. This is due to IPsec packets with an old replay counter. These error messages can be safely ignored.

10) When defining Office Mode IP pools, make sure each cluster member has a distinct pool.

11) When detaching a cluster member from a VPN cluster, manually remove the VPN domain once the member has been detached.

12) If a VPN-1 High Availability cluster is handling a connection from a Remote Access VPN-1 Client located on the same subnet as the cluster and fails over to another cluster member occurs, the connection with the VPN-1 Client may be terminated.

13) When based on topology information, the VPN domain calculation contains only the cluster member topology and not the cluster object topology. This may cause errors in the VPN domain of clusters since the cluster object and members may have different subnets. In this case, define the VPN domain manually on the cluster object. This issue does not exist on VSX appliances.

**VPN Hardware/Software Acceleration**

14) VPN-1 accelerator cards will not offload the encryption tasks if SecureXL is installed on the same machine. In this scenario the card can still be utilized for public key operations.

15) SecureClient using Office mode, when connecting to a Load Sharing cluster with SecureXL. Multiple interfaces feature for Office mode may not route outgoing packets properly, and connections may be disconnected as a result. In order to prevent this from happening you can activate IP compression for the client.

16) To enable IKE acceleration on a Nokia platform with a Nokia Encryption Accelerator card installed, use the following IPSO CLI command: `set pkcs11-checkpoint register`. Currently, you cannot use Voyager to enable IKE acceleration.

**IKE, Interoperability**

17) Clarification: The global property **Support Authentication methods: Pre-shared Secret**, under **Remote Access -> VPN - Basic** tab, applies only for the use of pre-shared secret with aggressive mode in IKE phase 1. However, the user's pre-shared secret, which appears in the **IKE Phase 2 Properties window** of a user object, is used for following additional purposes, which are not affected by the above property:
   1. IKE Hybrid mode with pre-shared secret for user authentication.
   2. For L2TP termination (used by Microsoft IPSec clients) with MD5 challenge.
   3. SSL authenticated topology download (not over IKE) for SecuRemote/SecureClient.
NAT with VPN

18) The use of the option that disables NAT (in the community) is applicable to hide NAT and not to static NAT.

19) Using Static NAT on the destination of a SIP connection inside a VPN-1 tunnel is not supported.

VPN-1 diagnostics (logging, monitoring, planning)

20) When using the IP pools NAT mechanism for gateway-to-gateway connections, no log is available for the IP assignment.

21) If you are working on SecureXL and VPN-1, reports on traffic may display inaccurate values.

22) When a host inside the encryption domain tries to open a back encrypted connection to SecuRemote/SecureClient, an Accept log instead of Encrypt shows up in SmartView Tracker.

23) An accept log may be received when using an SMTP resource with VPN even if the connection was encrypted.

24) When a user is configured on SmartCenter to work with encryption algorithm AES128, an inaccurate reject log entry appears in SmartView Monitor that can be safely ignored stating: Client Encryption: the user is not defined properly. However, the connections establishment succeeds.

L2TP Clients

25) Since Windows 2000 clients can open a single L2TP based VPN tunnel concurrently, it is not possible to maintain L2TP connection with two VPN-1 Modules concurrently. This may create problems when the VPN module is a CPLS cluster configuration.

   Workaround: In order to work with L2TP in load sharing configuration, configure the CPLS cluster to place each connection in the same gateway.

26) When using L2TP for remote access VPN Drop logs may be received due to traffic sent from the L2TP client, with the following Information fields:

   • encryption failure: received a cleartext packet within an encrypted connection received when cleartext packets arrive from the physical IP of the client
   • encryption failure: Cannot identify peer for encrypted connection received when the destination is either broadcast or not part of the encryption domain.

   These logs can be safely ignored.

27) When Microsoft IPSec VPN client (using L2TP) connects to a VPN-1 gateway, the connection will be counted twice, which will be reflected in the counter of concurrent Remote access VPN tunnels in SmartView Status and in the SmartView Monitor.
28) Using Microsoft IPsec/L2TP clients behind hide NAT where VPN-1 Net cluster is the destination gateway and DHCP is in use for Office Mode is not supported.

29) When using Microsoft IPsec/L2TP clients for Remote Access VPN, routing traffic to destinations other than the encryption domain of the VPN-1 Gateway (for example to the Internet or to another destination in the VPN) is not supported.

**Nokia Clients Support (CryptoCluster & Symbian)**

30) Nokia clients are not supported when the gateway side is a load-sharing cluster configuration; unless you follow the instructions outlined in the *Clustering Configuration Guide for IPSO 3.8* which explains how to establish VPNs with non-Check Point gateways and clients. This document can be downloaded from the Nokia customer support site (https://support.nokia.com).

**VPN-1 and SecuRemote/SecureClient Issues**

31) The combination of using multiple external Interfaces (route through different interfaces) for SecuRemote/SecureClient and clusterXL pivot mode is not supported.

32) When connecting with a VPN-1 client to a VPN-1 cluster, the message "tunnel test failed" may appear on the client side; however, connectivity between the client and the gateway is not impaired.

**Miscellaneous**

33) When using the command `cprestart` on the SmartCenter Server, it will not apply to the VPN-1 Module. In order to restart the VPN-1 Module, run `cpstop` followed by `cpstart`.

34) When configuring VPN persistent tunnels, configuration remains after using the command `cprestart`. In order to overcome this issue use `cpstop` and then `cpstart`.

35) **Dynamic IP resolution** is not supported in Traditional Policy mode, if under a rule's Encrypt properties **allowed peer gateway** is enabled.

**VPN-1 Edge/Embedded**

**VPN-1 Edge/Embedded Clarifications and Limitations**

**Policy Installation**

1) If you have VPN-1 Edge/Embedded profiles or SmartLSM Edge/Embedded profiles, when you create a new policy file, be aware that SmartDashboard will not warn you that the new policy is also defined on profiles that were previously installed with another policy. Instead, define specific targets per policy file.

2) Groups with exclusion are not supported on VPN-1 Embedded/Edge rules.

3) Using the RTSP service with VPN-1 Edge/Embedded is not currently supported.
4) For SMP customers or customers who upgraded from NG with Application Intelligence (R54) and used the SSC, the Profile Hi-Med-Low_Profile is combined from three policy targets that can be used in the Install On column. However, those targets are not included in the generic Policy Targets object. To workaround this, specify the High, Medium or Low targets themselves in the Install On column. Otherwise if installing it on Policy Targets, they will not have any effect on the VPN-1 Edge/Embedded appliance.

5) When defining VPN-1 Edge/Embedded appliances to perform VPN as Remote Access, avoid placing the appliance's profiles on the rule's destination cell.

6) Slow policy installation that eventually fails may occur when no DNS is configured on your SmartCenter Server. Either define DNS (in the following order: resolution of files, DNS and then NIS), or contact Technical Support.

7) When using the group All VPN-1 Embedded devices defined as Remote Access on the rulebase, the icon that is defined is wrong and can be safely ignored.

8) When using rules with resources, avoid installing them on VPN-1 Edge/Embedded profiles. Resources are currently not supported with VPN-1 Edge/Embedded appliances.

9) The Reboot option is currently not supported when upgrading firmware.

VPN-1 Communities

10) Do not use the SmartDashboard feature that allows adding VPN-1 Edge/Embedded objects to the Remote Access community as Participating Gateways. The appearance of this option will be removed in the future.

Logging

11) VPN-1 Edge/Embedded gateways support only regular log tracking. When using other tracking at a rule that would be installed on such gateways (profiles) they are ignored.

12) Logs from VPN-1 Edge/Embedded do not show the rule number.

13) The VPN-1 Edge/Embedded implied rule for SWTP_SMS and SWTP_Gateway protocols does not generate logs so you will not see logs for these connections.

Platforms

14) VPN-1 Edge/Embedded can be managed if the SmartCenter is running on either Windows 2000, Solaris2, Linux or SecurePlatform. In addition, if exporting from one of the supported platforms and then importing to one of the non-supported platforms, the global property support_sofaware_profiles must be set to false using DBEdit tool.

15) VPN-1 Edge/Embedded products cannot be managed from a Windows 2003 server.
**SmartUpdate**

16) The `uninstall` function is not currently supported when updating firmware using SmartUpdate.

**SmartView Status**

17) After installing a Security Policy on a VPN-1 Edge/Embedded Profile the status of the corresponding VPN-1 Edge/Embedded gateways is displayed as `unknown` until the next time the gateways connect to the SmartCenter Server for periodic updates.

It is possible to force the VPN-1 Edge/Embedded gateway to connect to the SmartCenter Server for updates, from the web portal of the appliance.

**SecuRemote/SecureClient**

SecuRemote/SecureClient has no separate release for NG with Application Intelligence (R55) for IPSO 3.8. Please refer to the NG with Application Intelligence (R55) for specific information regarding SecuRemote/SecureClient.

**SmartUpdate**

**SmartUpdate Clarifications and Limitations**

**License Management**

1) Use SmartUpdate to delete central licenses. CPConfig supports only local licenses and cannot be used to manage central licenses. You can also do this operation using the `cplic del` command line from the Check Point Gateway machine.

**Product Management**

2) SmartUpdate supports managing licenses but does not support managing products from a Nokia SmartCenter Server.

3) Using SmartUpdate to perform a remote upgrade to NG with Application Intelligence with IPSO (R55) for IPSO 3.8, is not supported.

**SmartView Monitor**

**SmartView Monitor Clarifications and Limitations**

**Installation**

1) SmartView Monitor has a central licensing scheme. It is no longer necessary to attach licenses to modules. Licensing is controlled exclusively by the SmartCenter Server. SmartView Monitor services are provided with other licenses such as: SmartView, SmartCenter Pro and FloodGate-1 modules.

If you do not have one of these bundles you can purchase and install either:

- SmartView for single Gateway/Module *or*
- SmartView for unlimited Gateways/Modules
2) When upgrading a Version 4.1 FloodGate-1 Gateway, to continue using the traffic monitoring features, in addition to upgrading FloodGate-1, install SmartView Monitor on the gateway.

**General**

3) Enabling SmartView Monitor Traffic history reports has some performance impact on the module. It is suggested not to enable it on Gateways that have 100Mbps throughput or higher.

4) To remotely control a 4.1 Real-Time Monitor module from a NG with Application Intelligence SmartCenter Server, use only the SmartView Monitor's SmartConsole Client and not the command line.

5) When editing or adding objects (Network Objects, Services etc...) in SmartDashboard, install the Security Policy in order for the SmartView Monitor to apply the changes.

6) When monitoring traffic in real time for traffic passing through a FireWall-1 resource, traffic will be seen as the following: On the incoming interface there will be seen traffic originating in the client and destined to the FireWall-1 Gateway. On the outgoing interface the traffic will be seen as if it is originated from the original client and destined to the desired server.

7) SmartView Monitor history tables will not be updated if you change the module’s system time substantially backward. To work around this problem you need to stop the module and run a utility that will clean the tables of records that still have later time than the current time. To do this perform the following steps:

   a. run `cpstop -fwflag -proc`
   b. run `"upgrade_persistency -clean"
   c. run `cpstart`

8) **SmartView Monitor** is the current name (in the products column) for what was previously called **Real-Time Monitor (RTM)** in versions NG FP2 and before. Modules that are NG FP2 and below are referred to, in **SmartView Tracker**, as **RTM**.

9) If you select a Gateway as a **Source** or **Destination** to Filter or Group by, only the gateway’s main IP address is considered. If you want to include all of the gateway’s IP addresses, add them manually via the **Custom IP** dialog box.

**Virtual Link Monitoring**

10) To enable Virtual Links you must make sure your Security Policy allows the **E2ECP** service to be accepted on the external interfaces of the desired modules.

11) A DAIP Module cannot be an end point of a Virtual Link.
12) When configuring a Virtual Link with an Externally Managed gateway, it is now required that both gateways should be aware of each other. To create this awareness, configure the local gateway on the external SmartCenter and install policy on the other gateway.

13) A cluster cannot be defined as one of the end points of a Virtual Link.

**Configuration Specific**

14) A module running SecureXL is not supported for traffic monitoring in the SmartView Monitor.

15) On a Nokia platform, SmartView Monitor does not support Flows. Traffic passing through the Flows mechanism cannot be monitored by SmartView Monitor. Type the command `ipsofwd slowpath` on the Gateway's console to deactivate Flows.

**SAM**

16) A Suspicious Activity Monitor (SAM) rule will fail for a remote gateway if the SmartCenter Server is also a FireWall-1 module and no policy has been installed on it since adding the remote gateway.

**SmartView Reporter**

**SmartView Reporter Clarifications and Limitations**

**Minimum Hardware Requirements**

The following minimum hardware requirements were designed so that SmartView Reporter Server will be able to process a volume of about 3 GB logs per day and generate reports according to the performance numbers limitation. If you have less logs produced per day you can use a machine with less CPU or memory. This may cause degradation in the performance numbers. In addition, if your machine has less physical memory you will need to change the database cache size. To do this follow the instructions in “SmartView Reporter” User Guide under the section Changing the SmartView Reporter Database Cache Size.

1) The minimum hardware requirements for installing SmartView Reporter are:

<table>
<thead>
<tr>
<th></th>
<th>Windows</th>
<th>Solaris</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Processor</strong></td>
<td>Intel Pentium III</td>
<td>UltraSPARC IIi</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td>1000 MHz</td>
<td>400 MHz</td>
</tr>
<tr>
<td><strong>Disk space</strong></td>
<td>Installation 60MB</td>
<td>Installation 100 MB</td>
</tr>
<tr>
<td></td>
<td>Database 40 GB</td>
<td>Database 40 GB</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>1 GB</td>
<td>1 GB</td>
</tr>
</tbody>
</table>

**Hardware Recommendations**

- Configure the network connection between the SmartView Reporter Server machine and the SmartCenter or the Log server, to the optimal speed.
- Use the fastest disk available with a high RPM (revolutions per minute).
• Increase the machine's memory. It significantly improves performance.
• The SmartView Reporter Server machine should have a UPS.

**Minimum Software Requirements**

2) For Internet Explorer use at least 5.5 or higher. For Netscape Communicator use at least 6.2 or higher.

**Configuration**

3) For SmartView Reporter installs on Solaris, install the X11 font sets and Motif that are included in the Solaris distribution.

4) SmartView Reporter supports SmartCenter High Availability with some limitations:
   • SmartView Reporter Server should be installed on a machine separate from the High Availability SmartCenter machines.
   • SIC is established with between SmartView Reporter Server and the active SmartCenter machine.
   • All modules send their logs to a Log Server. The Log Server can be either one of the SmartCenter machine, or a separate machine.

   After performing change over:
   • Log consolidator will continue working and processing log files from the Log Server machine.
   • You need to re-initiate the SIC on the SmartView Reporter Server machine with the new active SmartCenter.

   After re-initiating SIC, SmartView Reporter Server will resume its work, and the SmartView Reporter client can connect to the new active SmartCenter.

5) If you would like to install SmartView Reporter Server on an existing Log Server machine, run the following commands after the SmartView Reporter installation completes:
   a. cpstop
   b. cpd_config -a Lcutild lutilid_addon register_lcutild_addon
deregister_lcutild_addon
c. cpprod_util CPPROD_SetValue "Reporting Module" "ManagementEnhancement" 4 0 1
d. cpstart

6) When a SmartView Reporter Server's IP address is statically NATed, a machine running the SmartView Reporter Client must be able to route connections to the real SmartView Reporter server's IP address. This can be achieved by running the SmartView Reporter Client on a machine in the Server's local network, or sometimes, by adding the appropriate route entries in the SmartView Reporter Client's routing table.
7) FTP or HTTP distribution of reports does not work with proxy settings. If a your machine has proxy settings, use alternate distribution methods such as e-mail distribution or copy files from the Report's Results directory instead.

**General**

8) Account logs that originated by a gateway cluster, are counted twice. Thus, reports of these logs will display inaccurate data.

9) The SmartView Reporter user interface only supports password-based login.

10) Logs produced by FireWall-1 modules that also have Floodgate-1 installed, show twice the number of actual HTTP connections. As a result, reports generated on such modules will display an incorrect number of connections.

11) When the log consolidator is working on the active log file, `fw.log`, the Management tab shows the progress of the consolidation. However, when either a automatic or manual log switch occurs, it is not indicated in the Management tab. The log consolidator continues processing the active log file.

12) On rare occasions, the log consolidator may pause when “Starting” for a long time. This situation can occurs after a power shutdown of the SmartView Reporter Server machine or when restarting the log consolidator after it has reached an “aborted” state due to exhausted disk space.

Therefore, always keep the database with enough disk space to avoid such problems.

13) When the SmartView Reporter has been deactivated on the IPSO platform, the SmartView Reporter client cannot function. If you open your SmartView Reporter client to an IPSO SmartCenter with a deactivated SmartView Reporter server, you will not see reports in the GUI. Clicking any menu from SmartView Reporter's GUI results in an error message: An internal error has occurred in SmartView Reporter. All changes will be lost and the SmartView Reporter client closes. If you encounter this issue, activate the SmartView Reporter on the IPSO SmartCenter.

14) Processing the detailed URL information inside the logs consumes a lot of resources. By default, this processing is therefore disabled. Extended URLs and file extensions are not available by default. To enable URL processing to run on your SmartView Reporter Server machine run:

a. the `cpstop` command

b. the `log_consolidator -K true` command

c. the `cpstart` command

After enabling URL processing, go over your web activity and FTP activity reports, and select all the sections that display detailed URL-related information. The sections (in the above reports) that are influenced are as follows:
a. Top Pages
b. Top Pages and their top sources
c. Top Files
d. Top file types.

If you wish to disable the detailed processing of URL information inside the logs again run:

a. the \texttt{cpstop} command
b. the \texttt{log\_consolidator -K false} command
c. the \texttt{cpstart} command

15) The Netscape browser does not print generated reports correctly and only displays them correctly from Netscape version 6.2 or greater. Netscape could not handle page breaks correctly. Instead, print the report with a version of Internet Explorer 5.5 or greater.

\textbf{SmartLSM}

\textbf{SmartLSM Clarifications and Limitations}

\textbf{General}

1) To enable SmartLSM support and to start the SmartLSM SmartConsole, run the commands \texttt{LSMenabler on} and \texttt{cpstop/cpstart} on the SmartCenter Server.

2) SmartLSM supports status monitoring of up to 1000 gateways from a single SmartCenter Server. The rest of the gateways receive the status \textit{Waiting}.

3) To support High Availability of SmartCenter servers, define both SmartCenter servers from SmartDashboard > \textbf{Profile Object} > \textbf{Logs and Masters} > \textbf{Masters} tab.

4) In SmartLSM, when removing a Dynamic Object from the list of Centrally Resolved Dynamic Objects and executing a \textbf{Push Dynamic Objects} action, the previous values of the removed Dynamic Object are not eliminated from the ROBO Gateway. The elimination of these values will be done the next time the ROBO Gateway performs a periodic policy fetch. You can invoke \textbf{Push Policy} (either instead of \textbf{Push Dynamic Objects} or afterwards) to correctly eliminate them.

5) In Windows, the caret character (^) is ignored when you input it from the command line. Do not use it in object names. For example: "aa^aa" is treated as "aaaa".

6) All actions in SmartUpdate are not supported for Profile Objects. Do not try to perform these actions.

7) After converting a ROBO gateway to a Corporate Office gateway, or converting a Corporate Office gateway to a ROBO gateway make sure you restart the Check Point services (or reboot) on the gateway. Also make sure to install policy on all the rest of the Corporate Office gateways.
8) SmartLSM does not support VPN-1 routing for satellites using the **To center and to other satellites through center** option.

9) You should not create objects in SmartDashboard with names of ROBO Gateways objects.

**SmartLSM SmartConsole**

10) When a critical notification is received and the **Action** tab is open, the critical icon blinks in order to get your attention. Stop the blinking by opening the **Critical Notification** tab. It may happen that after a critical notification has been received and the icon is blinking, the critical status is then changed and the critical record is removed before you had the chance to open the **Critical Notification** tab. In this scenario, the icon will continue to blink but no record will be displayed when opening the **Critical Notification** tab.

**Installation and Configuration**

11) After defining the interfaces of a ROBO gateway through **cpconfig**, you must perform **cprestart** or fetch the policy for the new definitions to catch.

**Policy Configuration**

12) **Uninstall Policy** from a Profile object has no meaning. Uninstalling a profile will result in error. You can safely ignore this error.

13) Resolve all Dynamic Objects that are used in the policy. An unresolved Dynamic Object will result in dropping all the packets that match the other characteristics of the rule.

**ROBO Gateway**

14) Before trying to pull a certificate from the SmartCenter server, configure the DNS Server settings in the ROBO gateway.

15) In **cpconfig** running on a ROBO Gateway, the text for pulling a SIC Certificate from the SmartCenter Server refers to a Dynamic Address Module. Enter the ROBO Gateway Object name as defined in SmartLSM.

16) SmartLSM ROBO gateway on Nokia is only supported with IPSO version’s 3.5 and 3.7.

**SecureXL**

**SecureXL Clarifications and Limitations**

**Unsupported Products**

1) FloodGate-1 is not supported with SecureXL or for Flows acceleration.

2) SmartView Monitor is not supported with SecureXL.
3) PPTP and PPPoE interfaces are not supported by SecureXL in configurations where NAT and/or VPN-1 are used.

Unsupported Features
4) The Overlapping NAT feature is not supported with SecureXL.

ClusterXL
ClusterXL Clarifications and Limitations

General
5) When installing a Policy failover may occur. To avoid this enable a "freeze" mechanism that prevents some actions that caused member to restart. By default this mechanism is disabled.

To enable this mechanism run the following command:
fw ctl set int fwha_freeze_state_machine_timeout 30

To disable this mechanism run the following command:
fw ctl set int fwha_freeze_state_machine_timeout 0

Configuration
6) When the FireWall-1 services on one or more cluster members are stopped using the command fwstop, policy installation on the cluster will cause the installed policy to be inconsistent between the active and stopped members. To make sure that the installed policy is always consistent across all members use the cpstop command instead of the fwstop command.

7) The following error messages may appear on the console when enabling or disabling the ClusterXL or State synchronization from cpconfig.
FW-1: fwkdebug_register: module cluster already registered
FW-1: fwha_kdebug_register: fwkdebug_register failed

These messages may be safely ignored.

8) Use the cpstop and cpstart commands instead of cprestart in cluster configurations. Using cprestart may lead to an unstable cluster state.

9) On the IPSO platform, in order to work with a third party cluster (a.k.a state synchronization) you must work in a Nokia VRRP or Nokia IP Clustering configuration. In order to work with other third party products (such as external load balancers) you can work around the restriction mentioned above by configuring IP Clustering with an empty IP Cluster. Just enter the cluster ID (same on all machines) and an administrative password. This is done through a Nokia Configuration Tool (such as Voyager).
VPN-1 Clusters

10) When adding a gateway (that belongs to a VPN community) to an existing cluster:
   a. first remove that gateway from the community
   b. then add a gateway to the desired cluster
   c. then add the cluster to the VPN community that this gateway belonged to prior to step a.

11) When detaching a cluster member from a VPN cluster, manually remove the VPN domain once the member has been detached.

12) When defining Office Mode IP pools, make sure each cluster member has a distinct pool.

13) Peer or secure remote gateways may show error messages when working against an overloaded gateway cluster in load-sharing mode. This is due to IPsec packets with an old replay counter. These error messages can be safely ignored.

14) When based on topology information, the VPN domain calculation contains only the cluster member topology and not the cluster object topology. This may cause errors in the VPN domain of clusters since the cluster object and members may have different subnets. In this case, define the VPN domain manually on the cluster object. This issue does not exist on VSX appliances.

High Availability

15) Issuing a Stop Member command in SmartView Status performs the `cphastop` command on this member. Among other things this disables the State Synchronization mechanism. Any connections opened while the member is stopped will not survive a failover event, even if the member is restarted using `cphastart`. However, connections opened after the member is restarted are normally synchronized.

Load Sharing

16) Traceroute through any load sharing cluster may fail.

17) Under load, **tcp packet out of state** error messages may appear. For each one of the cases there is a specific way to resolve it. Refer to the “FireWall-1 SmartDefense” documentation for a full explanation and security implications.

   a. `message_info: TCP packet out of state · first packet isn't SYN tcp_flags: FIN-ACK`  
      `message_info: TCP packet out of state · first packet isn't SYN tcp_flags: FIN-PUSH-ACK`

      In SmartDashboard > Global Properties > Stateful Inspection, enlarge **tcp end timeout**. The recommended value is 60 seconds. If there are many connections consider enlarging the connection table size in the same ratio as the **tcp end timeout**.

   b. `message_info: SYN packet for established connection` run the command: `fw ctl set int fw.trust_rst_on_port <port>` When a single port is not enough, you can set the port number to -1, meaning that you trust a reset from every port.
c. Other out of state messages: run the command: `fw ctl set fwconn_merge_all_syncs`.

This allows a more reliable way of merging tcp states across asymmetric connections.

**Authentication**

18) When using automatic or partially automatic client authentication for HTTP on CPLS clusters (both ClusterXL and OPSEC clusters), define a decision function based only on IP addresses in order for connections to open.

From the **Gateway Cluster Properties > ClusterXL > Load Sharing >Advanced >select IPs** (the third radio button).

Defining a decision function on OPSEC clusters products is done via the individual product. Refer to the individual product's documentation for more information.

19) When performing manual client authentication (using port 900) to a cluster where the members' IP addresses are not routable, the URLs returned in the HTML from the replying cluster member contain the member's own non-routable IP address instead of the cluster IP address. This fails subsequent operations. The workaround is to configure the cluster to use a domain name instead of an IP address in the client authentication HTML pages, using the `ahttpclientd_redirected_url` global property. Make sure that your DNS servers resolves this domain name to the cluster's IP.

**State Synchronization**

20) Only one synchronization network can be defined per subnet. Use different subnets if more than one synchronization network is defined.

**SmartConsole**

21) When working with a third Party Cluster object with FloodGate-1, if you move from the **Topology** tab to a different tab the following errors message appears: **No interface was activated in QoS tab for this host (Inbound or Outbound). Do you want to continue?**

Select Yes and continue your operation. This error message can be safely ignored.

22) SmartUpdate shows Cluster members as distinct Gateways without the common Cluster entity. When cluster members are not of the same version, applying **Get Check Point Gateway Data** on a cluster member will set the member's version on the Cluster object. To set the version of the cluster correctly, apply the **Get Check Point Gateway Data** command to the cluster member with the latest version.

**Security Servers**

23) Security Servers are not supported with Sequence Verifier in Load Sharing Cluster environments.

**Services**

24) When using T.120 connections, make sure you manually add a rule that allows T.120 connections.
FloodGate-1 Clarifications and Limitations

SmartCenter Installation
1) When installing a SmartCenter Server, you should specifically select the FloodGate-1 product in addition to selecting the SmartCenter product. Selecting FloodGate-1 is required in order to manage FloodGate-1 modules.

SecureXL
FloodGate-1 is not supported with Flows. When FloodGate-1 is enabled, Flows acceleration is disabled. FloodGate-1 is not supported with SecureXL. Run `cpconfig` in order to choose between the two products.

Platform Specific - Nokia
2) In order to use FloodGate-1, activate the product in Voyager, then re-login as administrator using the terminal and perform `cpstop` then `cpstart`.
3) On Nokia, FloodGate-1 and VPN-1 Pro are two separate packages. When upgrading VPN-1/FireWall-1 from 4.1 to an NG with Application Intelligence, make sure to upgrade FloodGate-1 as well. After the upgrade, FloodGate-1 is disabled by default. Use Voyager to turn on FloodGate-1.

Clusters
4) It is not possible to convert a FloodGate-1 gateway into a cluster member if this gateway appears in the Install On column in the rule-base. To resolve this:
   a. Remove the FloodGate-1 gateway from the Install On column.
   b. Convert it into a cluster member.
   c. Add the member to the Install On column in the relevant rules.
5) When editing the Topology tab of a Cluster Object from Type third party, the following message can be safely ignored: "No interface was activated in Qos tab for this host (Inbound or Outbound). Do you want to continue?" On a third party cluster, the QoS topology related definitions should be edited on the cluster member object.

Low Latency Queuing (LLQ) and DiffServ
6) When managing QoS Classes, there is an option to define new DiffServ Class of Service Group. This option is not valid and should not be used.
7) The values Inbound Guaranteed and Outbound Guaranteed for the Best Effort class in the table DiffServ and Low Latency classes in the QoS tab of the Topology window may be inaccurate when adding a Low Latency class or a DiffServ class to the interface. Since this error does not affect the correct scheduling of FloodGate-1, it can be ignored.
8) In the QoS Rule Base, although it is possible to paste an LLQ class before a DiffServ class, it should not be done.

URI

9) Matching connections will fail to be correctly classified, in cases where you are using Authenticated QoS and URI for QoS in the same QoS rule.

Logging

10) Sub rules do not inherit the log track from the parent rule. To overcome this issue, add the Log/Account track to the specific sub rule you want to log.

11) Under heavy load, FloodGate-1’s accounting might lose the some of the connection parameters such source/destination. Please ignore those account records.

Authenticated QoS

12) The Authenticated QoS feature uses the UserAuthority Server to get user authentication data. Before using this feature, refer to the UserAuthority Server section for the list of its known limitations.

Miscellaneous

13) FloodGate-1 may not schedule traffic on an interface that was newly enabled on the gateway. In order for the interface to be recognized by FloodGate-1, run the command cprestart.

14) Despite the message, deactivating an interface direction for QoS in the object topology does not remove it from the Install On column in the rule base. To overcome this issue, manually remove the interface direction from the Install On column.

UserAuthority

UserAuthority Server Clarifications and Limitations

Installation

1) Installation of UserAuthority Server NG with Application Intelligence on Terminal Server or Citrix machine, may fail if the machine is not connected to the network.

General

2) While running in Legacy Mode, UserAuthority Server does not support WebAccess encryption options in trust (e.g, you cannot enforce VPN encryption by using UserAuthority WebAccess trust).

3) When using UserAuthority Server in a High Availability Cluster when failover occurs the UserAuthority Server on the standby still maintain it's UAA session with all clients (such as UserAuthority WebAccess) although it is no longer the active server. The workaround is to: run both the uagstop and uagstart commands on the standby module when failover occurs.
4) Routing configurations in which a destination can be reached through multiple interfaces with the same metric is not supported. The Citrix UAS identifies connections by a 4-tuple: source port, destination IP and destination port. The source IP is not taken into account. As a result the Citrix UAS cannot differentiate between concurrent connections that differ by their source IPs only. For example, if the two following connections are opened simultaneously:

<table>
<thead>
<tr>
<th>User</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe</td>
<td>192.168.0.3</td>
<td>5001</td>
<td>209.81.7.23</td>
<td>80</td>
</tr>
<tr>
<td>Bob</td>
<td>192.168.0.2</td>
<td>5001</td>
<td>209.81.7.23</td>
<td>80</td>
</tr>
</tbody>
</table>

Then the UAS does not guarantee that the right user identification will be returned for queries on those two connections.

5) UserAuthority Server. When changing Trusted Domains (under Global Properties > UserAuthority) from All Domains to Specific Domains, some users may be required to re-enter credentials to UserAuthority WebAccess in Web Single Sign-On scenario.

6) When using a log server, a Security rule which allows ELA traffic from the UserAuthority Server to this log server, should be explicitly defined.

7) When users are authenticated on other VPN-1 Pro gateways using Client Authentication, SecureClient or SecuRemote, the automatic configuration isn’t able to resolve the connection to the username.

8) UserAuthority Server NG with Application Intelligence supports two modes on the Solaris, Linux or Nokia platforms:
   - Legacy - which has UAG FP3 functionality
   - New - which has additional capabilities, such as integration with Windows Group etc.

To check the mode - run "uagmode stat" from $UAGDIR.

To switch the mode - run "uagmode new" or "uagmode legacy"

**OPSEC**

**SmartCenter**

1) In CPMI the command line `fw unload` does not trigger an `eCPMI_NOTIFY_UNINSTALL_POLICY` notification event.

2) An OPSEC application that reads logs using LEA supports up to 1000 log files (*.log and *.adtlog). If more are needed, move the log files from $FWDIR/log to another directory.

3) An OPSEC application that reads logs using LEA may fail if the network objects database contains more than 2000 objects.
4) A Suspicious Activity Monitor (SAM) rule will fail for a remote gateway if the SmartCenter Server is also a FireWall-1 module and no policy has been installed on it since adding the remote gateway.