

# SofaWare Security Management Portal 7.0 Release Notes

December 2007 – Revision 3

---

## TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>3</b>
<b>Highlights of This Version .....</b>	<b>3</b>
<b>Availability.....</b>	<b>3</b>
<b>Copyright.....</b>	<b>3</b>
<b>More Information .....</b>	<b>3</b>
<b>UPGRADING FROM PREVIOUS VERSIONS .....</b>	<b>4</b>
<b>From SMP 7.0 Early Availability Version.....</b>	<b>4</b>
<b>From SMP 6.0.....</b>	<b>4</b>
<b>From Earlier Versions .....</b>	<b>4</b>
<b>Upgrade Notes .....</b>	<b>5</b>
<b>KNOWN ISSUES.....</b>	<b>7</b>
<b>CHANGES BETWEEN SMP 6.0 AND SMP 7.0.....</b>	<b>8</b>
<b>SMP Virtual Portals (SMP Instances) .....</b>	<b>8</b>
<b>Security &amp; User Management.....</b>	<b>12</b>
<b>Usability .....</b>	<b>12</b>
<b>Logging.....</b>	<b>14</b>
<b>Platform Support .....</b>	<b>15</b>
<b>Gateway Management.....</b>	<b>15</b>

<b>Firmware Updates .....</b>	<b>17</b>
<b>Notifications.....</b>	<b>17</b>
<b>Reporting .....</b>	<b>18</b>
<b>SMP API .....</b>	<b>18</b>
<b>VPN Management.....</b>	<b>18</b>
<b>Web Filtering Service .....</b>	<b>20</b>
<b>Centralized Email Filtering Service .....</b>	<b>20</b>
<b>SUPPORTED PLATFORMS .....</b>	<b>21</b>
<b>Server Platforms .....</b>	<b>21</b>
<b>Embedded NGX Appliances .....</b>	<b>21</b>
<b>OPSEC Partners .....</b>	<b>21</b>
<b>Web Browsers.....</b>	<b>21</b>
<b>SYSTEM REQUIREMENTS .....</b>	<b>22</b>

## Introduction

SofaWare Security Management Portal (SMP) provides a scalable method of configuring and controlling anywhere from a few Embedded NGX gateways to hundreds of thousands of Embedded NGX gateways and for delivering add-on subscription security services, such as Dynamic VPN, Dynamic DNS, reporting, automatic updates, Web Filtering, Email Filtering, VStream Antivirus signature updates, and Vulnerability Scanning. SMP is specifically designed for the scalability and high availability needs of service providers and large enterprises.

This document contains the summary of changes between SMP 6.0 and SMP 7.0.

## Highlights of This Version

SMP 7.0 incorporates a host of new and improved features, including:

- Revamped Virtual Portals
- Granular Permissions
- Global System Administrators
- Enhanced User Interface
- Built in web filtering service

## Availability

SMP 7.0 is available to SMP customers with a valid software subscription contract.

## Copyright

© Copyright 2007 SofaWare Technologies Ltd.

SofaWare is a registered trademark of SofaWare Technologies Ltd.

Check Point is a registered trademark of Check Point Software Technologies Ltd.

## More Information

For additional information, technical support, and assistance see:

<http://www.sofaware.com/support/>

## Upgrading from Previous Versions

### From SMP 7.0 Early Availability Version

To upgrade from the SMP 7.0 Early Availability Version to the SMP 7.0 General Availability version, run the SMP 7.0 installer on the server where SMP 7.0 EA is installed. The installer will automatically upgrade the previous installation.

You must perform the upgrade in-place.

### From SMP 6.0

#### Upgrade Process

There are two upgrade options from SMP 6.0:

- In place upgrade.
- Upgrade on a new server.

To perform an in-place upgrade, run the SMP 7.0 installer on the server where SMP 6.0 is installed. The installer will automatically upgrade the previous installation.

To perform an upgrade on a new server, run “SMP Backup” on the old server running SMP 6.0. Then, on the new server, start the SMP installer, and select “Install from backup” in the “Setup Type” page. Select the backup file created by SMP 6.0.

#### Deleting Recovery Data

During upgrade to SMP 7.0, some recovery data is maintained in the database, to allow recovering from fatal errors during installation.

After a successful installation, you may want to free up database space consumed by the recovery data. To delete the recovery data, run the utility “smp\_cleanup.bat”.

### From Earlier Versions

To migrate from earlier versions of SMP, first upgrade to SMP 6.0, then upgrade from SMP 6.0 to SMP 7.0 GA as described above.

## Upgrade Notes

### Licensing

Upgrading to SMP 7.0 requires a new license key. Existing SMP customers with a valid support/software subscription contract can obtain a new license key by contacting SofaWare support.

### Supported Firmware

To support some new features of SMP 7.0 GA, firmware version 7.5 or higher must be installed on the Embedded NGX appliances.

Older firmware versions are supported, but certain new features of SMP 7.0 may be ignored by gateways running firmware older than 7.5.

### Old Logs Cleared

Due to improved logging format, all log messages will be cleared upon upgrade.

### Templates Reset To Default

Upon upgrade, customized report templates will be reset to the new default format and settings.

On upgrade, the old templates are automatically backed up to the following path:  
\$SMP\_HOME\SMP6\backup\templates\<portal-name>

### Global Administrator

During the upgrade process, a new global administrator account will be created. To this end, you will be prompted to choose a new username and password.

### Administrators Converted To Users

Upon upgrade, all the administrators defined in the system will be converted to users. These users' administrative roles and permissions will be preserved.

### Upgrading a Multiple-Instances Installation

When upgrading from an SMP 6.0 installation with multiple instances (virtual portals), the SMP global configuration will be taken from the first instance.

Note: when upgrading a multiple-instances installation, only a single server group can be defined. Prior to running the SMP7 installer, ensure that no more than one server group is defined.

### **DVPN Downtime**

When upgrading from SMP6, the CA is re-initialized. This may cause several minutes temporary VPN downtime. The Dynamic VPN communities will resume normal operation after the CA is re-initialized.

### **SMP API Changes**

The SMP API has been significantly improved in this version. Due to these changes, client applications using older versions of the SMP API may require slight modifications. For more information, refer to the SMP 7.0 programmer's guide.

## Known Issues

The following known issues exist in SMP 7.0 GA:

### Installer

ID	Summary
16444	When upgrading from SMP 6.0, if the previous SMC version is lower than 6.0.46, non Latin (Unicode) characters in customer names may be converted to “?”. <b>Workaround:</b> Prior to upgrading to SMP 7.0, install SMC 6.0.46. For complete instructions, contact SofaWare.
15184	Installer fails to configure SMP while using non-Latin characters in privileged user's name. <b>Workaround:</b> Do not use non-Latin characters in the username.
16150	In certain cases, the Microsoft .NET framework installer displays a warning message during installation, regarding a missing EULA.txt file. <b>Workaround:</b> This warning can be ignored.
16199	When upgrading from SMP6 with multiple instances defined, using “From backup” mode, the virtual portal to IP address mapping are not migrated. <b>Workaround:</b> Use “In Place” upgrade mode.
16636	After upgrading from SMP6, in certain cases, no portals are visible, and only the system menu is visible. <b>Workaround:</b> Clear the web browser cache. This will correct the display.

### SMC

ID	Summary
15519	Internal Networks are not remotely managed when Internet port is assigned to one of the LAN ports locally on the appliance. <b>Workaround:</b> Reassign the Internet port to “WAN” prior to connecting the gateway to SMP.
13278	DNS names with underscores are allowed by SMP, but are not supported by the DNS standard, and such names do not work as expected in Internet Explorer 7. <b>Workaround:</b> Do not use underscores in gateway names.

16180	Export and import do not support all the VSS (Vulnerability Scanning) settings.
13549	SMP incorrectly allows creating VLANs for gateway types that do not support VLANs.

## SMS

ID	Summary
16626	When SofaWare UFP Server is enabled for the first time, it will take a while to download the URL category database (~ 160MB) from the Internet. Until this initial download process is completed, all web sites will be categorized as “Allowed”.

# Changes between SMP 6.0 and SMP 7.0

## SMP Virtual Portals (SMP Instances)

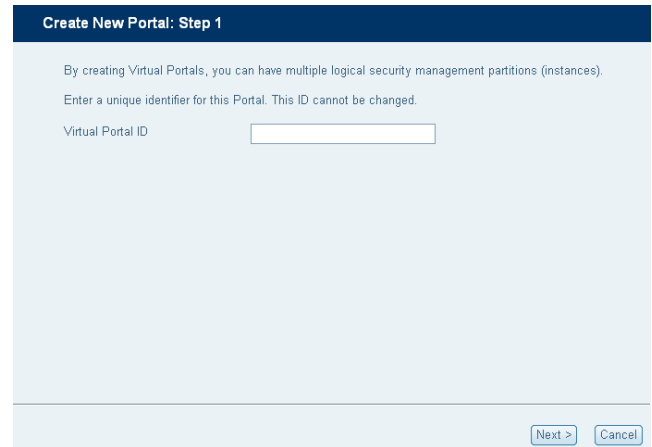
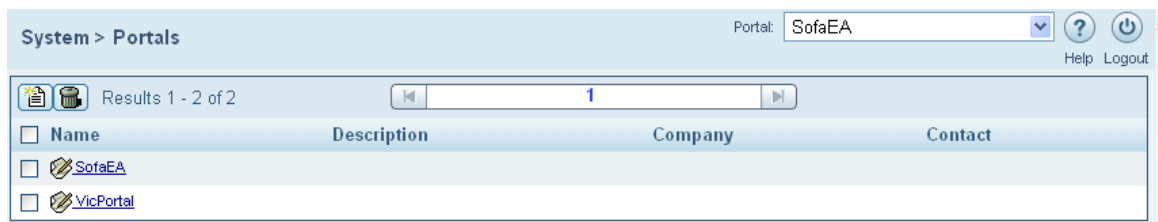
### Terminology Change

In SMP 7.0, the term “SMP virtual portal” replaces the term “SMP instance”.

### Improved Virtual Portal Creation Process

SMP 7.0 includes a wizard that allows system administrators to create new SMP virtual portals directly from the SMC Web interface. If needed, portals can also be deleted through the SMC Web interface.

This means that you no longer have to run the SMP installer in order to create a new portal or remove an unneeded portal.

Name	Description	Company	Contact
<input type="checkbox"/> SofaEA			
<input type="checkbox"/> VicPortal			

## Portal Contact Details

Each SMP virtual portal can be associated with a set of contact details, including company, contact person, email address, and description.

Configure View License Edit License Name: vicportal Actions

General

Enter the details of this portal.

Description: Industrial automation portal

Company: Acme Ltd

Contact: Albert Yin

Email: alberty@acme.com

## Global System Administrators

SMP 7.0 offers two categories of user accounts: *users* and *system administrators*.

*System administrators* have global access to all virtual portals defined in the system and can switch between them instantly using a special drop-down list. A system administrator can be granted either read-only or read-write permissions.

User ID	First Name	Last Name	Email	Phone	Type	Logged In
<input type="checkbox"/> smpadmin	smpadmin	smpadmin	m@n		Administrator	<span style="color: red;">●</span>
<input type="checkbox"/> victoria	victoria	victoria	victoria@tech-lav.com		Administrator	<span style="color: green;">●</span>

*Users* are defined per virtual portal, and can be granted flexible permission levels for elements in the relevant portal. For example, the following types of users can be defined:

- An end user with no administrative access, who can only receive notifications from the virtual portal
- A user with access to a VPN community defined in the virtual portal
- A user with read-only access to the virtual portal's SMC management interface
- A user with full administrative access to all objects in the virtual portal (a "Super User")

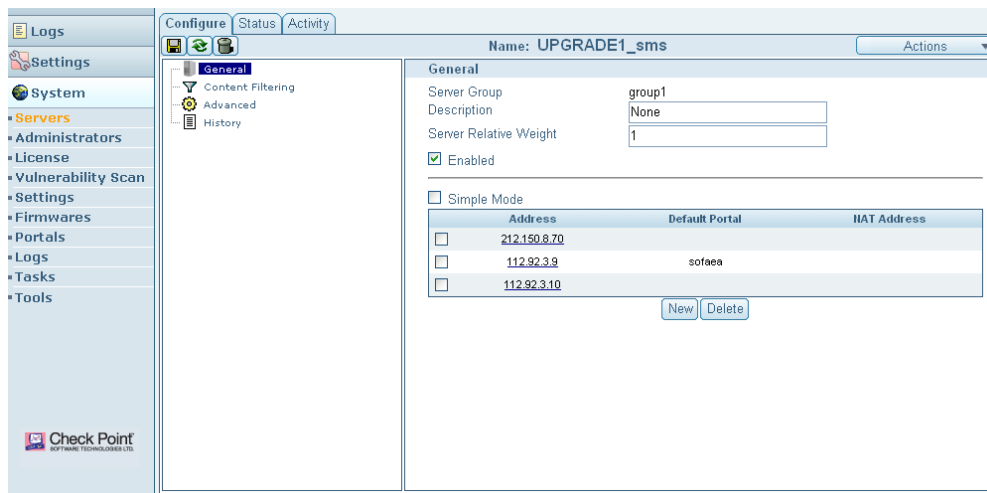
## Improved Virtual Portal Scalability

SMP 7.0 has been optimized to support a large number of virtual portals. Hundreds of virtual portals can be defined on a single server.

## Multiple Virtual Portals with a Single SMS IP Address

To lessen the complexity and cost of maintaining multiple IP addresses, it is now possible to use a single SMS IP address for multiple virtual portals.

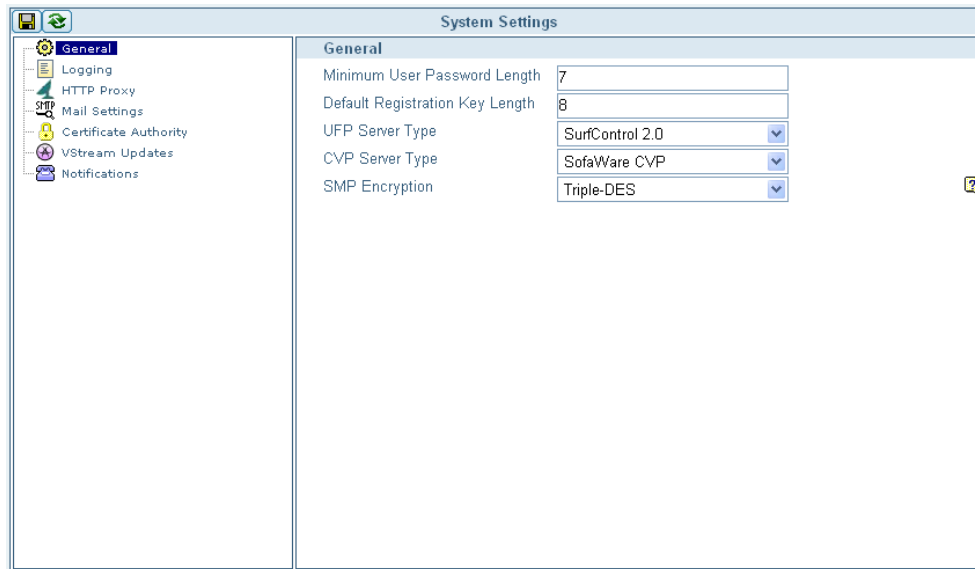
As in previous versions, it is still possible to assign a different IP address per virtual portal, if needed.



*Note: If multiple virtual portals share a single SMS IP address, you are required to use a non-ambiguous, fully qualified gateway ID when connecting the gateway to the Service Center. The format of the fully qualified gateway ID is “gatewayid.portalname”.*

## Global Settings

To reduce the complexity of managing an SMP installation that consists of many virtual portals, the global settings and tools in SMC are now shared between all portals in the system, and are shown under the “System” tab.

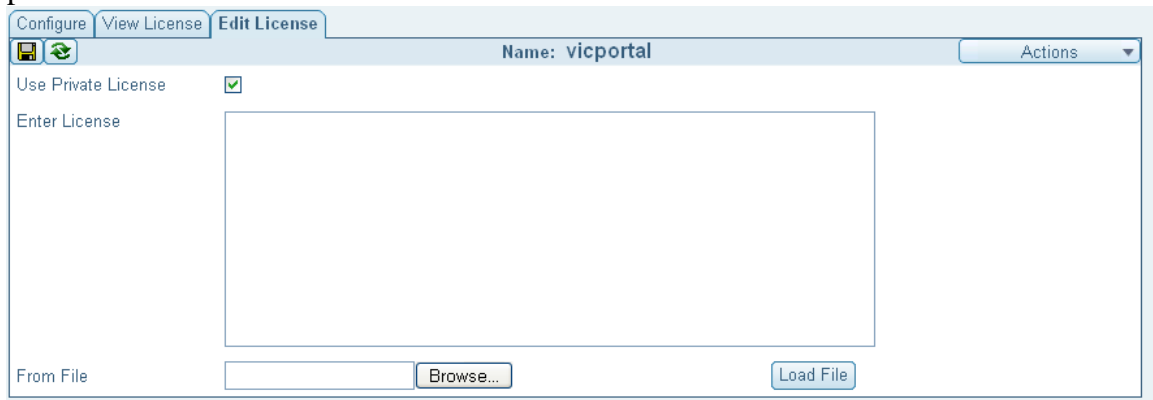


These settings and tools include:

- Firmware images
- System Settings
- VStream Antivirus updates
- HTTP proxy and email settings
- System logs
- Certificate Authorities
- Tasks list
- Import/export

## Global License

The system license is now specified globally and shared by all the defined virtual portals.



In addition, it is possible to specify a private license for individual virtual portals. A private license will override the global license.

## Security & User Management

### Fine-Grained User Permissions

SMP 7.0 offers a highly flexible role-based system for managing user permissions. System administrators create and customize user roles with a fine level of detail, specifying exactly which objects users of this role can view, edit, and create. The system administrators then assign each user to a role.

Name	Description
<a href="#">Community Manager</a>	Can manage all "End users" and gateways associated with this user's communities
<a href="#">End User</a>	Cannot login to SMC, and is not permitted to view or change any settings
<a href="#">Power User</a>	Can view and modify any object in this portal, except for roles and privileged users
<a href="#">Read Only User</a>	Can login and view all objects in this portal
<a href="#">Super User</a>	Can view and modify any object in this portal
<a href="#">Support User</a>	Can create and modify gateways and "End Users", and view all the objects in this portal

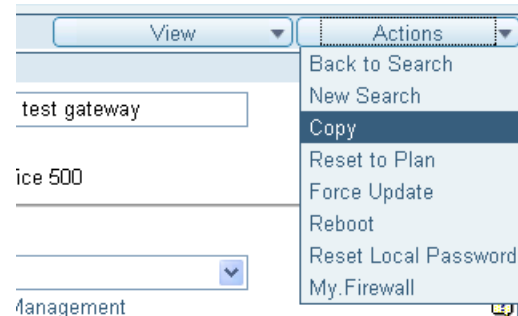
### Password Guessing Protection

SMP 7.0 includes protection against brute force password guessing attacks. If a user makes three incorrect login attempts within one minute, the SMC automatically prevents the user from attempting to log on for one full minute.

## Usability

### Gateway/Plan Copy Operations

SMP 7.0 allows system administrators to copy plans and gateways.



## New Wizards

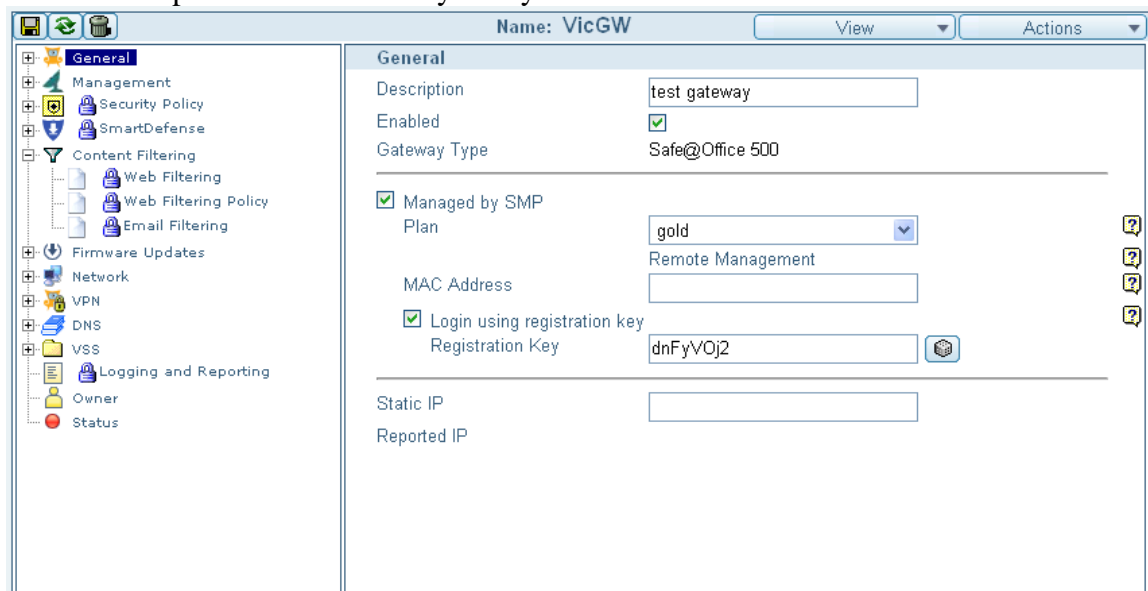
Several new, easy-to-use wizards guide the user through common procedures:

- Creating a new gateway
- Creating a new plan
- Creating a new user
- Creating a new community
- Creating a new server
- Creating a new server group



## Tree-Based Editors

Many of the SMC pages have been restructured and now include a new, tree-based navigation pane. This new format enables easier and more intuitive access to the multitude of parameters offered by the system.

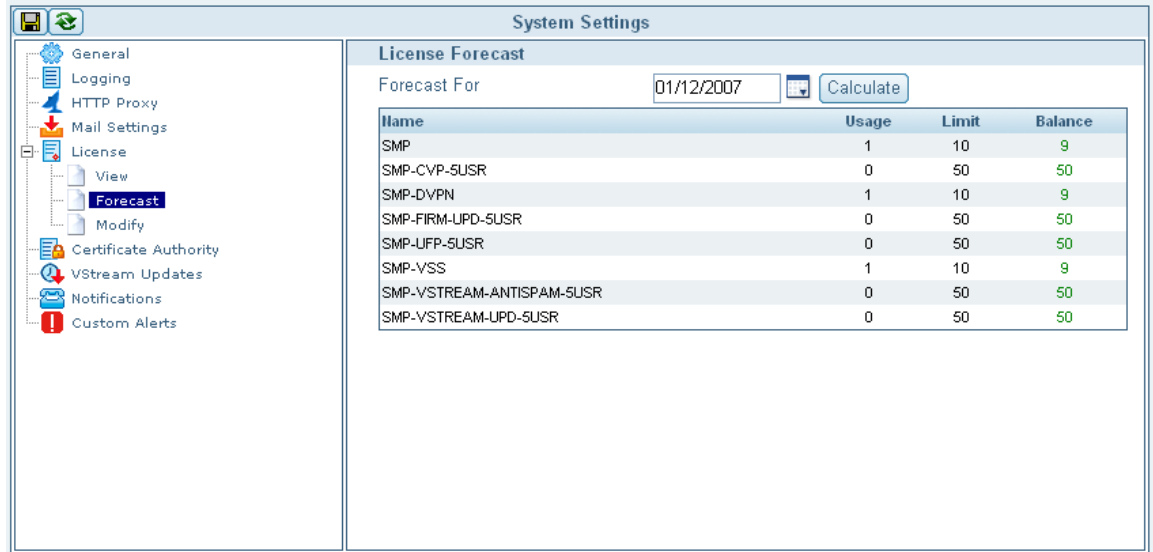


## Task Cancellation

The SMC **Tasks** report now allows the user to cancel selected tasks that are currently running.

## License Expiration Forecast

A new License Expiration forecast report enables an administrator to plan ahead the number of subscription items which need to be renewed by a specified date.



Name	Usage	Limit	Balance
SMP	1	10	9
SMP-CVP-SUSR	0	50	50
SMP-DVPN	1	10	9
SMP-FIRM-UPD-SUSR	0	50	50
SMP-UFP-SUSR	0	50	50
SMP-VSS	1	10	9
SMP-VSTREAM-ANTISPAM-SUSR	0	50	50
SMP-VSTREAM-UPD-SUSR	0	50	50

## Export Plan to Excel

Plans can now be exported to Microsoft Excel format.

## Logging

### Fault-Tolerant Logging

If the SMC is not accessible, the SMSs persistently buffer all received logs on the local hard drive, until the SMC comes back online.

### Enhanced Logs Format

Instead of a textual format, log messages are now stored and transferred in an efficient, compressed format.

The new format is approximately three times more efficient, both in disk space consumption and network bandwidth consumption. Furthermore, security report generation is now significantly faster.

### Enhanced Log Viewer

The log viewer's performance has been improved significantly. In addition, log messages are now presented in a clearer way.

Log messages can now be filtered by the origin or user fields, and a quick method has been added to view today's log messages for a specific gateway, user or administrator, directly from the properties page of the corresponding object.

## Platform Support

### **Solaris Support Removed**

Solaris platform support was removed in SMP 7.0.

### **Apache Removed**

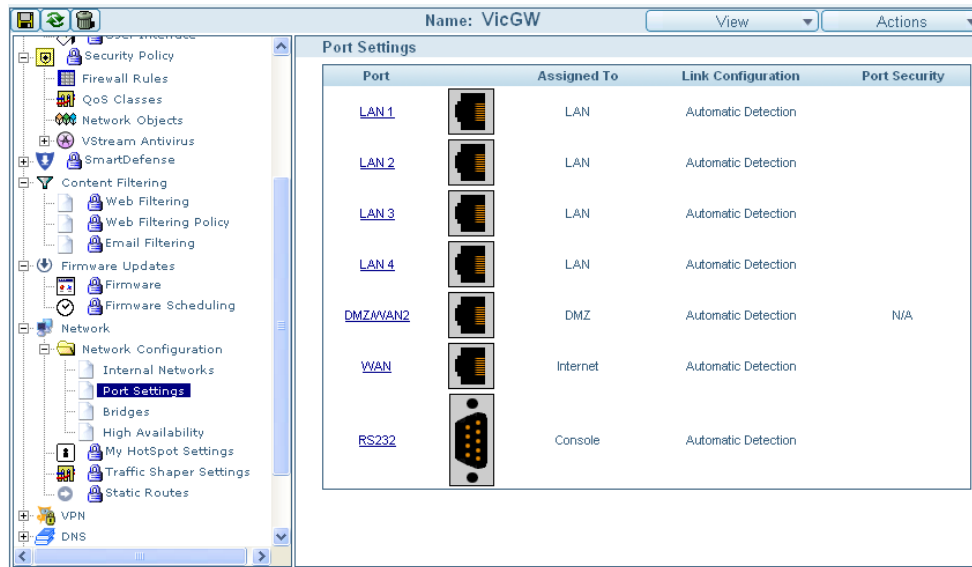
SMP 7.0 does not require an Apache Web server and does not install one.

## Gateway Management

### **New Managed Items**

The following items can now be managed from the SMC Web interface:

- Network Time Protocol (NTP) settings
- Gateway High Availability (HA)
- Fail-open option for Web Filtering / Email Filtering
- Bridges and bridge interfaces
- Flexible LAN port assignments
- New DHCP options supported in Embedded NGX firmware 7.0
- Wireless WPA encryption settings
- Time Based Security Rules
- Site-to-Site and Remote Access VPN sites
- Security rules with a specific VPN site in the source or destination.
- Allow & Forward Firewall rules with a specified destination IP address.
- Security Rule descriptions
- Service Objects
- Advanced NAT Rules
- Service based routes and Routes with specified destination interfaces.
- Web Rules
- Remote Desktop
- New SmartDefense protections: Checksum verification, URG flag clearing, TCP Sequence verifier, MSN messenger blocking.
- VStream Embedded Antispam (Requires firmware 8.0)
- Updated SmartDefense attack patterns
- "Nortel IP Phone" & "Avaya IP Phone" DHCP options.



## New Gateway Status

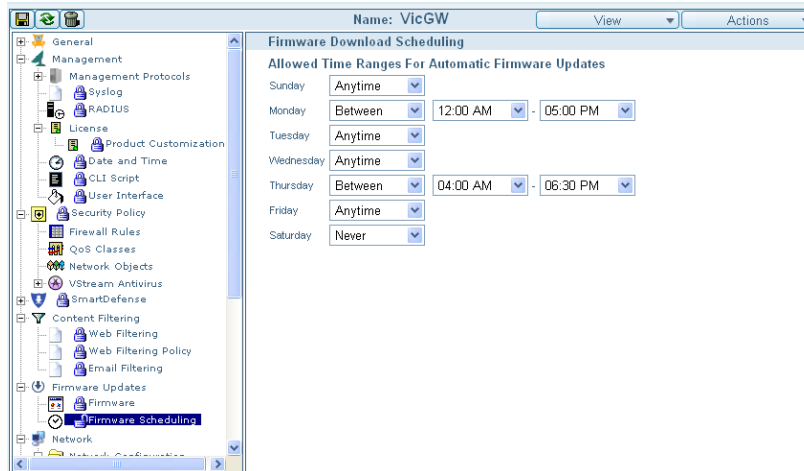
The following status items can now be displayed for each appliance:

- The currently installed VStream Antivirus database version
- The current local time on the appliance

## Firmware Updates

### Automatic Firmware Updates Scheduler

It is often preferable to perform automated firmware updates outside of normal business hours. To this end, SMP 7.0 enables administrators to set a schedule for firmware updates by specifying the hours and days of the week during which automatic firmware updates may take place. The schedule can be configured per plan or per gateway.



plan or per gateway.

It is still possible to trigger manual firmware updates outside of the scheduled hours, by selecting the gateway and clicking **Update Now**.

### ADSL Firmware Updates

SMP 7.0 supports updating ADSL module firmware images for Embedded NGX ADSL-enabled appliances.

ADSL module firmware images are now distributed as part of the \*.tgz format firmware packages, which can be obtained from the Check Point download center.

## Notifications

### Spam Sender Alert

A new alert allows notifying an antispam-enabled gateway's owner and selected system administrators, when the gateway detects a spam sender in the protected network.

### Quick Response to Gateway Disconnection

It is now possible to configure the "Gateway Disconnected" alert to be sent a specified number of minutes after the gateway's disconnection was detected. Previously, the report would be sent only after a full day of disconnection.

*Note: This feature should be used with caution. If the notification time threshold is set too low, unnecessary alerts may be sent when transient network failures occur.*

## Reporting

### Improved Report Templates

The security reports' default templates are now organized more efficiently and presented in a clearer way.

*Note: Upon upgrade to SMP 7.0, all customized report templates will be reset to the new default format.*

The report templates' syntax has been enhanced and made more consistent with the objects in the SMP SOAP/XML API.

### Virus Outbreaks Displayed in Administrator Security Report

The administrator security report now includes a viruses-by-date graph, allowing the administrator to view information about virus outbreaks.

### Administrator Daily Report

The system now allows emailing a daily administrator report. This report includes the following details:

- The list of gateways created today
- The list of gateways deleted today
- The list of gateways that connected today for the first time

## SMP API

### Improved Perl Installation

The Perl installation provided with SMP 7.0 includes all the modules required for using the SMP SOAP/XML API.

### Improved API

The SOAP/XML API has been enhanced for better clarity and updated to support all the new SMP 7.0 features.

## VPN Management

### Excluded Services

In SMP 7.0 VPN communities, it is now possible to select services handled in the clear (that is, services that will not be encrypted).

**Excluded Services**

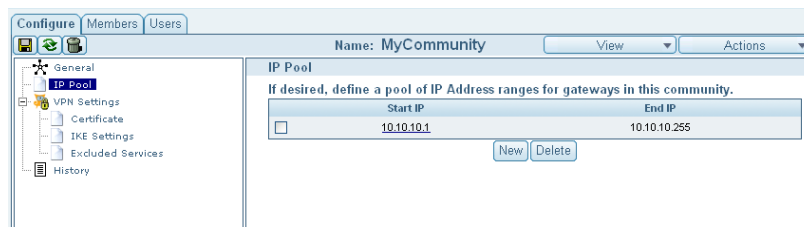
Define a list of services that are not to be encrypted

#	Protocol	Start Port	End Port
1	<input type="checkbox"/> UDP	90	91

## Automatic Network Address Assignment

When defining a VPN community, it is often desirable to assign non-overlapping private IP addresses to the community gateways, in order to ensure full connectivity between all the members in the community.

To simplify this task, SMP 7.0 allows defining a pool of IP addresses for each



community. When defining the networks of each individual gateway in the community, the administrator can then click the

**Suggest** button, to automatically select an unused IP subnet from the community's IP address pool.

## Permanent Tunnels

Normally, in SMP VPN communities, VPN tunnels are automatically established as needed, and closed when they are no longer in use.

In certain cases, it is desirable for the tunnels in a VPN community to remain permanently open, even during idle periods. To this end, SMP 7.0 allows enabling "permanent tunnels" for a community. Enabling this option ensures that all the tunnels in the community remain open at all times.

## VPN Tunnel Sharing

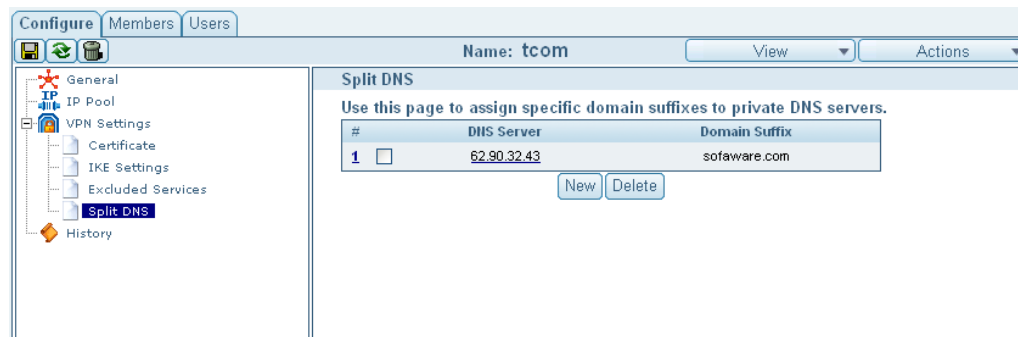
SMP 7.0 allows customizing the level of VPN tunnel sharing (IPSEC Phase-2 tunnels). The options are:

- One VPN tunnel per gateway pair
- One VPN tunnel per subnet pair

The default is "One VPN tunnel per gateway pair".

## Split DNS

Split DNS can now be configured on VPN communities. Split DNS allows directing DNS queries to the corporate domains to the corporate DNS server, while passing other DNS queries normally to the ISP DNS servers.



## IP Compression

The IP Payload Compression Protocol, or IPComp, is a protocol for compression of IP datagrams, described in RFC 2393. SMP 7.0 now supports enabling IP compression on a per-VPN community basis.

## Web Filtering Service

### SofaWare Integrated Web Filtering

SMP 7.0 now includes an integrated category based web filtering service, which is installed with each SMS (Security Management Server). When using the integrated web filtering service, a 3<sup>rd</sup> party UFP server is no longer needed.

### Websense 5.0 Supported

The Web Filtering service now supports the Websense 5.0 UFP server.

### UFP Server Redundancy and Load Balancing

It is now possible to define multiple external UFP servers, to be used for redundancy and load balancing.

## Centralized Email Filtering Service

### Updated SpamAssassin in SCS

The SpamAssassin version provided with the SCS has been updated to 3.1.8.

### Updated ClamAV in SCS

The ClamAV version provided with the SCS has been updated to 0.90.2.

### Disabling SMTP Scanning

SMP 7.0 allows system administrators to disable SMTP scanning for the centralized Email Filtering service, on a per-virtual portal basis.

Once disabled for a virtual portal, SMTP scanning will not be performed, regardless of whether it is enabled for a specific plan or gateway.

## Supported Platforms

### Server Platforms

SMP 7.0 supports the following platforms:

- Microsoft Windows 2000 Server (Intel)
- Microsoft Windows 2003 Server (Intel)

### Embedded NGX Appliances

SMP 7.0 supports the following appliances:

- Nokia IP30
- Nokia IP40
- Nokia IP60
- SofaWare S-box
- Check Point Safe@Office
- Check Point UTM-1 Edge X / W / S Series
- Check Point UTM-1 X Series
- Check Point ZoneAlarm Z100G
- NEC SecureBlade 300

*To support the full functionality of SMP 7.0, the Embedded NGX appliance must have firmware version 7.0.39 or higher installed.*

### OPSEC Partners

The following OPSEC partner applications are recommended for use with this release:

Antivirus:

- Trend Micro InterScan VirusWall
- Aladdin eSafe Gateway 4.0
- Computer Associates eTrust Antivirus version 7.1

Web Filtering:

- SurfControl SuperScout FireWall-1 edition
- Websense Enterprise

### Web Browsers

The following Web browsers are supported by SMP 7.0:

- Internet Explorer 6.0 or higher
- Netscape 7.1 or higher
- Mozilla Firefox 1.0 or higher

## System Requirements

<b>Item</b>	<b>Requirement</b>
OS	Microsoft Windows 2000 Server SP2 / Microsoft Windows 2003 Server
CPU	Pentium-III 1000 MHz or higher
Memory	1 GB recommended
Free disk space	5 GB minimum
File system	NTFS