



Premier Services Program (PSP) Tools: Deployment Guide

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
<http://www.extremenetworks.com>

Published: September 2008
Part Number: 100243-00 Rev. 03



Alpine, Alpine 3804, Alpine 3802, Altitude, BlackDiamond, BlackDiamond 6808, BlackDiamond 6816, EPICenter, Ethernet Everywhere, Extreme Ethernet Everywhere, Extreme Networks, Extreme Turbodrives, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, GlobalPx Content Director, the Go Purple Extreme Solution Partners Logo, SentiAnt, ServiceWatch, Summit, Summit24, Summit48, Summit1i, Summit4, Summit5i, Summit7i, Summit 48i, SummitRPS, SummitGbX, Triumph, vMAN, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Summit logos, the Extreme Turbodrives logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and other countries. Other names and marks may be the property of their respective owners.

© 2008 Extreme Networks, Inc. All Rights Reserved.

Specifications are subject to change without notice.

Merit is a registered trademark of Merit Network, Inc. Solaris and Java are trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Avaya is a trademark of Avaya, Inc.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org>).

This product contains copyright material licensed from AdventNet, Inc. (<http://www.adventnet.com>). All rights to such copyright material rest with AdventNet.

Use of Open Source Libraries. The Software uses or links to the third party "open source" library(ies). Please read the "Notice" files included with the Software for identification of these libraries and applicable license agreements.



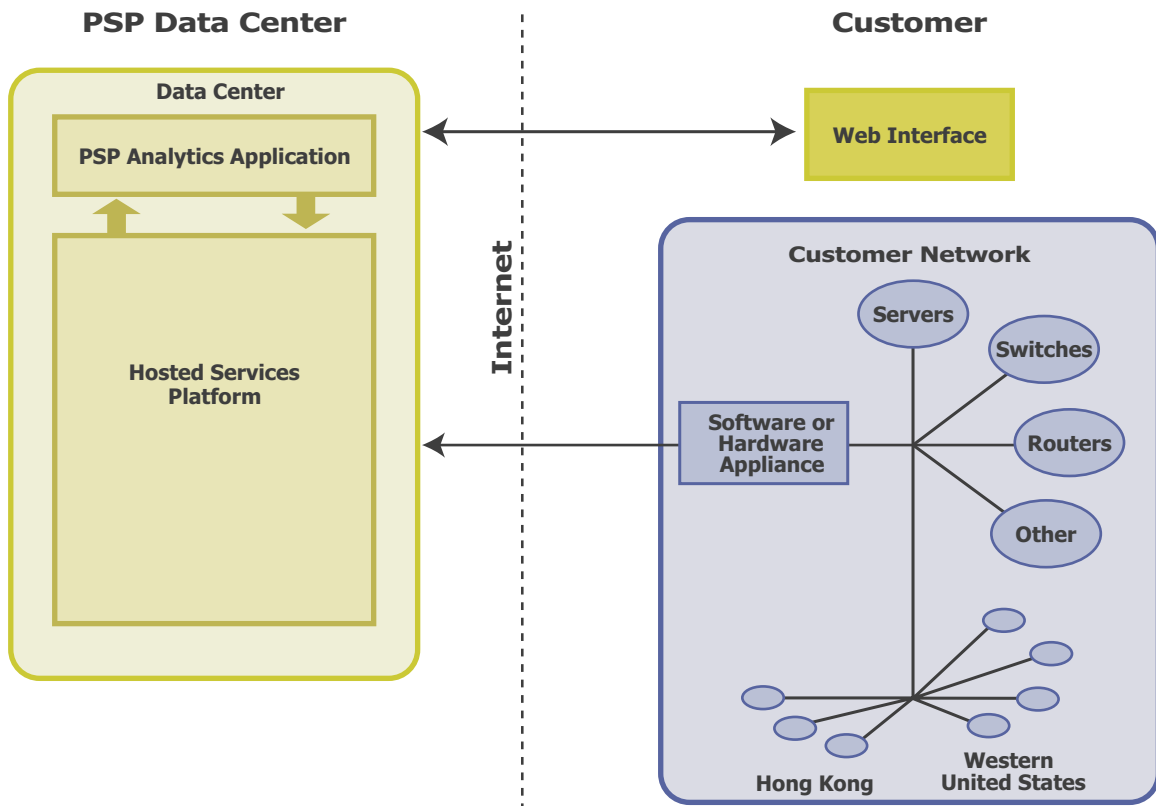
Contents

Chapter 1: Introduction to Premier Service Program (PSP) Tools	5
Chapter 2: Getting Started.....	7
Hardware and System Requirements	7
Software Set-up Instructions	7
Chapter 3: Configuring Network Devices.....	9
Example 1: Enabling SNMP on a Server Hosted by Windows Server 2003	9
Example 2: Enabling sFlow on an Extreme Networks Summit X450 Switch.....	12
Example 3: Enabling NetFlow on a Cisco Router	13
Chapter 4: Find/Add Devices	15
Device Configuration	15
Devices	16
New Devices	16
Edit Devices	16
Delete Devices	16
Interfaces.....	16
New Interfaces.....	16
Edit Interfaces.....	16
Delete Interfaces.....	16
Tunnels.....	17
New Tunnels.....	17
Edit Tunnels.....	17
Delete Tunnels.....	17
VIPs.....	17
Edit VIPs.....	17
Delete VIPs.....	17
Metrics.....	17
Activity Logging	18
eKPI Configuration	18
Configure PSP Cost eKPI Target Data	18
Configure PSP Cost Equipment Costs	18
Chapter 5: PSP Security	21
PSP's Secure Architecture	21
PSP Tools	21
PSP Interface	21
PSP Hosted Service.....	21
PSP Data Center	21
Chapter 6: PSP Software Implementation FAQ	23
Trademarks	23



1 Introduction to Premier Service Program (PSP) Tools

Extreme Networks provides an on-demand, hosted solution for monitoring and analysis of IT infrastructure, including network traffic, servers, and applications. The PSP Tools (software that resides on the monitored network) securely collect and transport data from a customer's network devices to the PSP Data Center, where it is analyzed and stored in the PSP database. The data is made available to end-users anytime and anywhere through a hosted Web application that provides drill-down analytics, role-specific dashboards, customized reporting, and sophisticated alerting.



This document provides comprehensive, step-by-step instructions for installing the PSP Tools on your network, establishing connectivity to the PSP Data Center, and performing the initial configuration required to begin using the PSP monitoring tools.

2 Getting Started

One of the advantages of the PSP tools is the ability to quickly deploy, install and configure our solution so you can gain insight into your IT infrastructure. Once the planning and information gathering steps are completed, a typical PSP deployment takes less than 30 minutes.

Your first steps are to complete the online registration process and review and accept the end user license agreement. You'll then receive a registration confirmation e-mail containing your registration key, a link to download the PSP Software and your user ID and temporary password.

- 1 Install the PSP software on a server meeting our minimum hardware requirements (listed below) by following the instructions in the installation wizard.
- 2 Open a Web browser and go to <http://extremenetworks.klir.com>. Click Customer Login and use your user ID and temporary password to log in to the PSP Portal. You will be directed to create a new password. The Quick Start link gives you access to information on getting started with PSP.
- 3 Also from Quick Start, you can Find and Add Devices, which will help you to discover and start monitoring assets on your network. After your network assets are enumerated in the PSP interface, it takes 5 minutes or less for configurations to update and performance data to become available.

At this point, your solution is up and running. You can take advantage of preconfigured dashboards, reports and alert templates to instantly begin analyzing and more effectively managing your IT infrastructure. Every interface leverages simple point-and-click capabilities, making PSP easy to use.

Any time you need assistance, refer to the Quick Start feature under the Help Menu in the upper-right corner of your PSP Analytics Web interface. If you need additional help, contact us at PSP@extremenetworks.com.

Hardware and System Requirements

Deploying the PSP software requires the following minimum hardware:

- Microsoft Windows® 2000 Server, Windows 2003 Server, or Windows XP Professional operating systems are supported. Windows 2003 and Windows XP Professional are recommended.
- 500 megahertz (MHz) processor, such as an Intel Pentium II or Advanced Micro Devices (AMD) processor. 1 gigahertz (GHz) processor or faster is recommended for best performance.
- 128 megabytes (MB) RAM. 512 MB recommended.
- 100 MB of Free Hard Disk space. 500 MB or greater for data caching.
- 10/100 Ethernet network adapter appropriate for the type of network you wish to connect to, and access to an appropriate network infrastructure with dedicated internet connectivity.

Software Set-up Instructions

To request the Software go to:

<http://extremenetworks.klir.com/register.html?campaign=727e6ed180b213b8bb559c522905f810>

The Registration Confirmation email contains a link to download the software installation file (*.msi) and a registration key.

- 1 Copy the installation file (*.msi) to a Windows server that meets the previously defined minimum specifications.
- 2 Open the installation file on the Windows server.
- 3 Follow the installation wizard instructions to complete the installation.
- 4 Go to <https://extremenetworks.klir.com> , login to the account using the temporary password, and follow the instructions to setup new devices for monitoring.

To complete the installation you will need the registration key contained in the Registration Confirmation email.



NOTE

TCP Port 443 must be open on your firewall to permit the software to securely encrypt and transfer data back to the centralized data center. Additionally, UDP Port 161 to monitored devices should be open to permit SNMP read-only queries by the software. If TCP Port 443 outbound is blocked on your firewall, but you are able to access HTTPS secure internet sites via an HTTP Proxy server, you can configure the software to connect through your proxy server.

The server should be situated and configured to provide IP access to all infrastructure that you intend to monitor. In the event of a highly distributed network environment (e.g. multiple WANs), or where more than 1,000 devices will be monitored, please contact PSP to receive additional registration keys and installation files for multiple installations of the software.

3

Configuring Network Devices

PSP requires Simple Network Management Protocol (SNMP) to be enabled on all devices that will be monitored. In addition, flow data collection requires that switches and routers be configured to send NetFlow (for Cisco® products) or sFlow® data to the PSP Software.

Specific steps required to enable SNMP, NetFlow, and sFlow vary depending on the device and operating system. You should refer to your manufacturer's documentation for specific instructions. Please contact PSP@extremenetworks.com if you have questions about configuring your network devices to work with PSP.

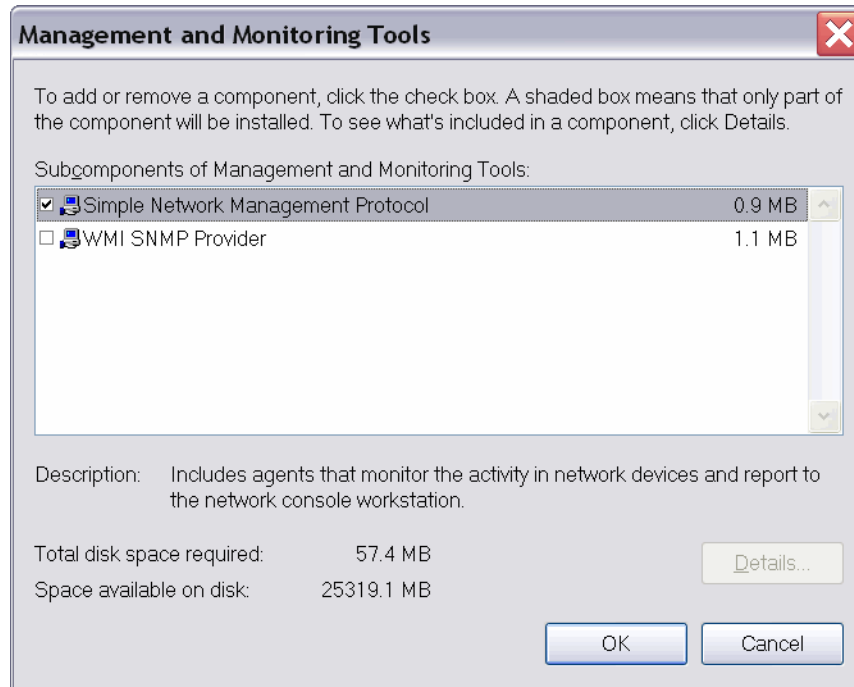
The following examples for enabling SNMP and sFlow are for demonstration purposes (actual configuration steps may vary):

Example 1: Enabling SNMP on a Server Hosted by Windows Server 2003

To enable SNMP on any server hosted by Windows Server 2003 (for example, Exchange Server), install and configure SNMP on Windows Server 2003.

To install SNMP on Windows Server 2003:

- 1 On the Start menu, point to Control Panel, and then click Add or Remove Programs.
- 2 In the navigation pane on the left, click Add/Remove Windows Components.
- 3 In the Components list, select but do not check Management and Monitoring Tools.
- 4 Click Details.
- 5 In the **Subcomponents of Management and Monitoring Tools** list, select the **Simple Network Management Protocol** check box.

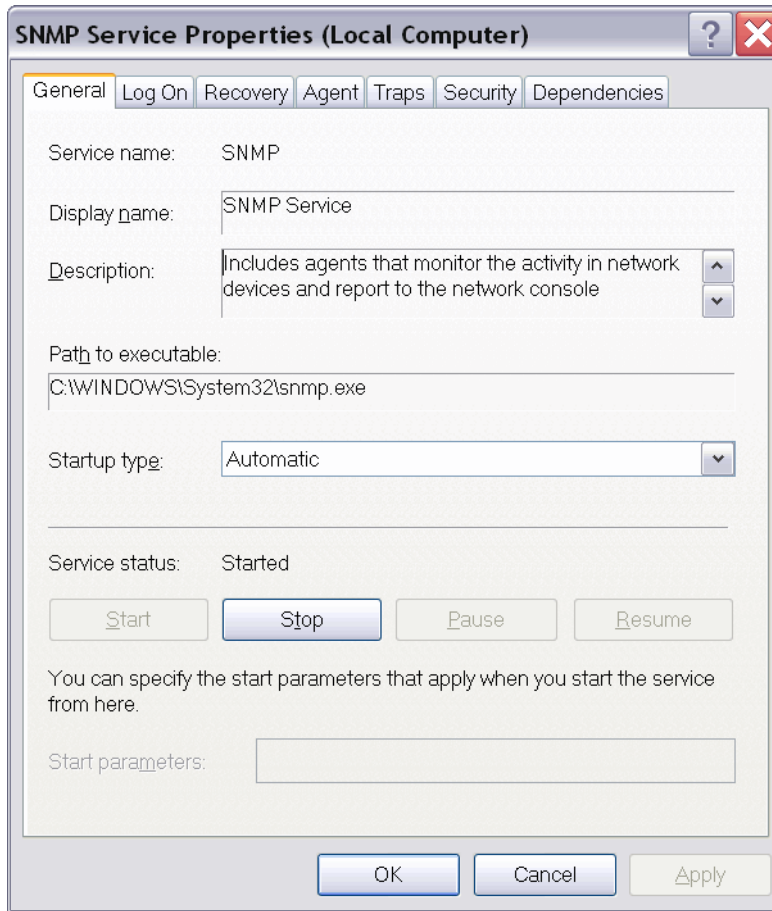


- 6 Click **OK**.
- 7 Click **Next**.
- 8 If prompted, insert a **Windows Server 2003 Installation CD** into your CD drive and then click **OK** (if a welcome screen for the installation CD appears, close it).
- 9 The **Configuring Components** page of the wizard will appear and indicate installation progress.
- 10 Click **Finish** and close the **Add or Remove Programs** dialog box.

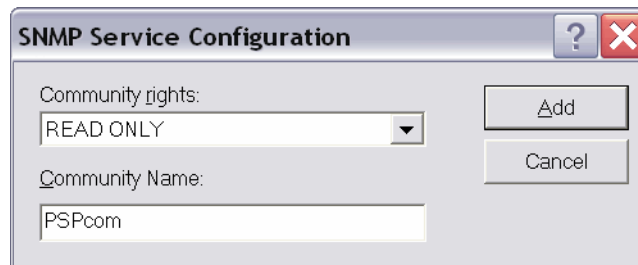
After SNMP is installed, the SNMP service will automatically start.

To configure SNMP:

- 1 On the **Start** menu, point to **Administrative Tools** and then click **Services**. The **Services** console appears.
- 2 In the details pane, right-click **SNMP Service**.
- 3 Click **Properties**.
- 4 On the **General** tab, confirm that the service is started. (if installed correctly, it is started during installation.)



- 5 If it is not started, in the **Startup type** box, select **Automatic** and then click **Start**.
- 6 On the **Security** tab, in the **Accepted Community Names** area, click **Add**.
- 7 On the **Community rights** menu, ensure that **Read only** is selected.
- 8 In the **Community Name** box, type a community name (for example, **PSPCom**).

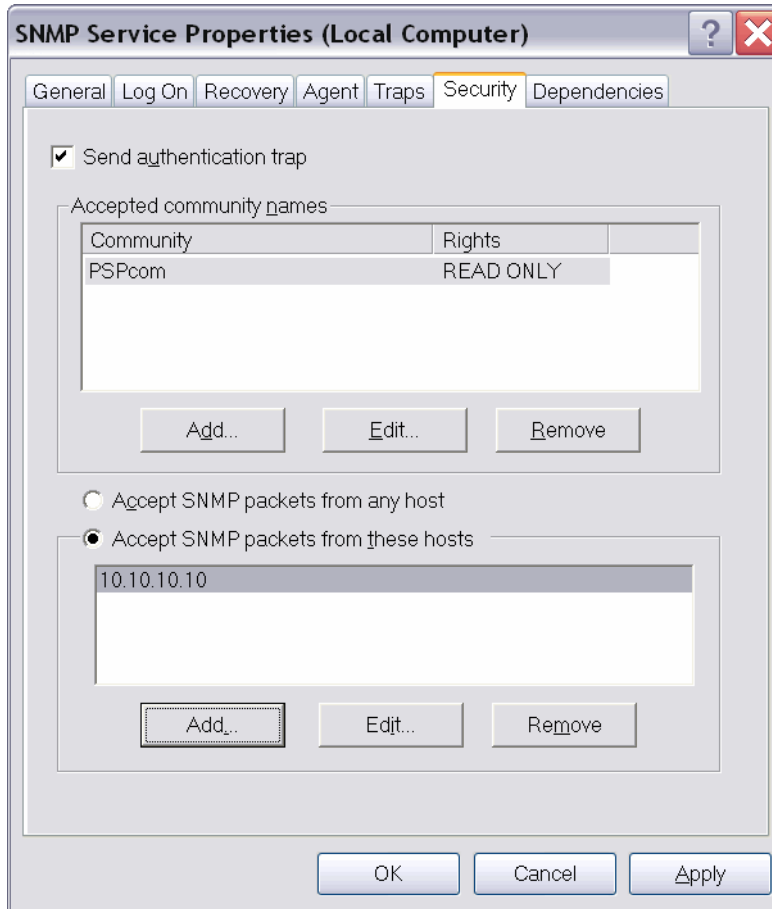


 **NOTE**

The community name serves as a password; devices making SNMP requests of the server will be ignored if they don't provide the correct community name.

- 9 Ensure that **Accept SNMP packets from these hosts** is selected, and then click **Add**. There are two Add buttons; click the lower one.

- 10 Type the IP address of the server where the PSP software is installed (for example, 10.10.10.10) and then click **Add**.
- 11 If you are using the high-availability configuration, enter the IP address of the secondary server where the PSP software is installed in the same way.



- 12 Click **OK**.
- 13 Close the **Services** console.

Example 2: Enabling sFlow on an Extreme Networks Summit X450 Switch

The following sFlow configuration example does the following:

- Configures the IP address of the sFlow data collector.

 **NOTE**

In many environments, the sFlow data collector is not directly connected to the switch. Make sure to specify the VR used to forward traffic between the sFlow collector and the switch. In most cases the VR is vr-mgmt.

- Configures the sampling rate on an edge port.

- Enables sFlow on the edge port.
- Enables sFlow globally on the switch.

```
configure sflow collector 55.55.55.69 vr vr-mgmt
configure sflow ports 4:12 sample-rate 1024
enable sflow ports 4:12
enable sflow
```

For further information, refer to the command reference and/or software user guides at <http://www.extremenetworks.com/services/documentation/swuserguide.aspx>.

Example 3: Enabling NetFlow on a Cisco Router

The following instructions explain how to enable NetFlow on a Cisco 3700 router running Internetwork Operating System® (IOS) 12.3. These instructions are only to illustrate the general process, and may not work in your environment.

To enable NetFlow on a Cisco router, run the following commands:

```
ip flow-export destination <VIP for high-availability appliance configuration,
appliance IP address for standard appliance configuration> 2055
ip flow-export version 5
ip flow-export source <interface name>
ip flow-cache timeout active 5
copy running-config startup-config
```

For example, a high-availability configuration using virtual IP address 10.254.0.99 and interface name FastEthernet0/0 would result in the following commands:

```
ip flow-export destination 10.254.0.99 2055
ip flow-export version 5
ip flow-export source FastEthernet0/0
ip flow-cache timeout active 5
copy running-config startup-config
```

To display the flow export settings, run the following command:

```
show ip flow export
```

Output similar to the following will appear:

```
Flow export v5 is enabled for main cache
Exporting flows to 10.254.0.99 (2055)
Exporting using source interface FastEthernet0/0
Version 5 flow records
0 flows exported in 0 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
```


4

Find/Add Devices

PSP allows you to discover devices on your network and add them to your account for monitoring. To begin select the software used to monitor devices on your network and establish the following search preferences:

- **Search By** - IP Address (one or more individual IP Addresses), Subnet Range (CIDR subnet range of IP addresses), Start/End IP Address (flexible setting of a subnet range based upon the starting and ending IP addresses)
- **SNMP Port** - (default 161) Port used by devices on your network to listen for SNMP requests.
- **SNMP Version** - (default 1) Version of the SNMP protocol used on the devices on your network.
- **SNMP Community** - (default public) String used to identify the SNMP Community profile of devices on your network.
- **After Discovery** - When “Install Devices Immediately” is selected, all devices that are discovered and are ready for installation will automatically be installed while all other discovered devices will appear in the Queue. On the other hand, if 'Add Devices to Queue' is selected, all devices that are discovered are added to the Queue.

As soon as these preferences are established, you may click the Find button to begin discovering devices on your network. If Install Devices Immediately is the selected After Discovery option, successfully installed devices will begin to appear under the 'Devices' tab, any other devices found will appear under the 'Queue' tab after refreshing the listing. If Add Devices to Queue is the selected After Discovery option, then all devices discovered will appear under the 'Queue' tab.

Devices in the queue may be installed if their installation status indicates they are ready to be installed. Select the devices you wish to install and monitor within PSP and click the Install button to begin the installation. The devices will soon appear on the Devices page as they become available.

Device Configuration

The Devices page consists of two listings:

- **Devices** - Installed devices that are currently being monitored within your account. Devices may include installed interfaces, VIPs, and tunnels.
- **Queue** - Discovered devices and interfaces that may be updated and installed for monitoring purposes.



NOTE

The 'Jump To' menu at the top of the Device Configuration page allows you to expand and collapse individual sections of the page for complete flexibility.

Devices

New Devices

You may add new devices to your account by discovering them with the Find/Add Devices Feature.

Edit Devices

You may make changes to one or more devices or queued devices using the Device Configuration page. Begin by selecting one or more items from the Devices or Queue tab and clicking the Edit button.

Delete Devices

You may remove Devices or Queue by selecting one or more devices from their respective tabs and clicking the **Delete** button.



WARNING!

When a user attempts to delete a device the system will present a warning message explaining that deleting an installed device will delete all historical data associated with that device. The user is required to acknowledge the warning before proceeding with the deletion.

Interfaces

New Interfaces

Find Interfaces allows you to find any additional interfaces that may have been added to a device after it was installed. Click on this button to be instantly presented with interfaces available on a device.

Edit Interfaces

You may make changes to interfaces of one or more devices, by selecting the interfaces from the Device Configuration page and clicking **Edit Interfaces**. When all desired changes are made, click **Apply Interface Changes**. Changes will not be saved until clicking the **Save** button at the bottom of the page.

Delete Interfaces

Interfaces may be deleted by selecting the interfaces you wish to remove and clicking the **Delete Interfaces** button.



WARNING!

When a user attempts to delete an interface the system will present a warning message explaining that deleting an interface will delete all historical data associated with that interface. The user is required to acknowledge the warning before proceeding with the deletion.

Tunnels

New Tunnels

Tunnels may be added to your account by clicking the **New Tunnel** button and establishing the tunnel attributes between two interfaces in your account.

Edit Tunnels

Tunnels may be individually edited from the Device Configuration page for either of the member devices for that tunnel. Select the tunnel you wish to edit and click the **Edit Tunnel** button.

Delete Tunnels

Tunnels may be deleted by selecting the tunnels you wish to remove and clicking the **Delete Tunnels** button.



WARNING!

When a user attempts to delete a tunnel the system will present a warning message explaining that deleting a tunnel will delete all historical data associated with that tunnel. The user is required to acknowledge the warning before proceeding with the deletion.

VIPs

Edit VIPs

VIPs may be individually edited from the Device Configuration page of the member device. Select the VIP you wish to edit and click the **Edit VIP** button.

Delete VIPs

VIPs may be deleted by selecting the VIP you wish to remove and clicking the **Delete VIPs** button.



WARNING!

When a user attempts to delete VIP the system will present a warning message explaining that deleting a VIP will delete all historical data associated with that VIP. The user is required to acknowledge the warning before proceeding with the deletion.

Metrics

When editing single installed items (devices, interfaces, tunnels, or VIPs) from the Device Configuration page, metrics may be detected or removed by selecting 'Yes' from the **Show/Edit Metrics** selection.

- To detect and add metrics, click the **Find New Metrics** button.
- To instantly remove metrics click the **Delete Selected Metrics** button.



WARNING!

When a user attempts to delete metric the system will present a warning message explaining that deleting a metric will delete all historical data associated with that metric. The user is required to acknowledge the warning before proceeding with the deletion.

Activity Logging

The **Activity Log** provides a historical change log of activity over the past 60 days of additions, changes, deletions made to devices in your account. You may filter results by user, and also sort by any of the columns listed in the log. The search capability allows for more granular data analysis.

eKPI Configuration

Configure PSP Cost eKPI Target Data

- 1 Modify PSP Cost eKPI target data by editing a device from the Device Configuration interface.
PSP Cost accounts have access to financial data linking equipment performance realization to actual costs (and unrealized costs).
Example:
The eKPI (Equipment Key Performance Indicator) is based upon a weighted formula that is indicative of equipment utilization and expressed on a scale of 0.0 to 1.0.
$$\text{eKPI (1.0)} = 45\% (\text{CPU Utilization}) + 35\% (\text{Traffic Utilization}) + 20\% (\text{Memory Utilization})$$

eKPI realization is then determined by dividing the eKPI by targets set by Users.
- 2 Enter the eKPI Target (with values ranging from 0.05 to 1.00.)
- 3 Click the **Save** button to update the device with the fresh eKPI settings.

Configure PSP Cost Equipment Costs

- 1 The Device Configuration page also provides PSP Cost accounts with the option of entering Purchase Price or Lease Cost, Maintenance contract price, and Labor costs.
- 2 Enter the Purchase, Lease, and Procurement details for the selected device.
If entering the Purchase method, select a purchase price and depreciation rate of Straight-line or Accelerated (Straight-line is default).
If entering the Lease Price, select the monthly lease cost and lease duration
- 3 Enter the cost for a Maintenance Contract, its procurement date, and the duration of the Contract.
The Contract Cost is calculated by dividing the Cost by the Duration of the Contract and adjusting to a monthly basis from the purchase date.
For mid-month purchase dates, the maintenance contract will be assumed to have commenced on the 1st or 15th of the month, rounded to the closest number. For example, a maintenance contract purchase on Jan 21 would be treated as having commenced on Jan 15; a maintenance contract purchased on Jan 29 would be treated as having commenced on Feb 1 of the following month.

- 4 Enter the labor hours and hourly rate.
- 5 Click the Save button to update the device with equipment cost settings.

5 PSP Security

PSP's Secure Architecture

Building on our collective experience at some of the most heavily utilized sites on the Internet, we have employed industry-best practices to ensure your data and identity remain private and secure. Only statistical packet information and management data leave your network; your data never automatically leaves the network through the PSP tools.

PSP Tools

The PSP Tools leverage software deployed at a customer's location to collect, encrypt and securely transport data from monitored devices inside your firewall. From the PSP software to the PSP Data Center, all data is secured using SSL/TLS authentication and encryption. Authentication is bidirectional, utilizing RSA 2048-bit X.509 certificates.

PSP Interface

To access data, customers log in through a secure Web interface, or https authentication, using 1024-bit X.509 certificates and encryption negotiated at up to 256-bit AES encryption, depending on the specific browser. The login or the entire session may be encrypted - either way, users are required to authenticate using a unique user name and password combination. Passwords are stored securely via secure hash algorithm (SHA), so no administrators or backend database administrators have access to stored passwords.

PSP Hosted Service

The PSP hosted service is secured with a combination of internal policies and network security measures. Rights management is restricted to the services and people that need it, and the entire platform is architected with 100% failover and redundancy at every layer on the stack. All data is backed up and archived regularly.

PSP Data Center

Limited access to the PSP Data Center ensures that the application servers are safeguarded inside a telecommunications-grade facility. Network security measures include the following: redundant commercial-grade firewalls, network address translation (NAT), IP masquerading (IPMASQ, which

makes all data appear to be coming to and going from the same IP address), and non-routable IP addressing.

The PSP Data Center is located inside a tier 1 telecommunications facility, which limits physical access to PSP's production environment. Physical security measures include continuous, manned security, biometric scanning, surveillance cameras, the KeyTrac™ system, and cardkey access. The PSP Data Center also employs redundant routing, smoke and particle sensors, dry pipe and sprinkler heads, and heat sensors to proactively identify and avoid events that could interrupt service. PSP regularly engages in internal security reviews and is constantly seeking to improve internal processes and procedures. If you have security questions, contact us directly at PSP@extremenetworks.com.

6 PSP Software Implementation FAQ

Q: We have a Web proxy. Can the PSP Tools still work?

A: The PSP software supports an HTTP Proxy using the HTTP CONNECT method for both Flows and SNMP. When entering connectivity settings during the installation dialog you will be presented with a checkbox option to enable HTTP proxy service for outbound network connectivity. Enter your proxy IP address, port number, authentication type (The PSP tools support HTTP basic or no authentication—Digest, NTLM, or custom authentication protocols are not currently supported), and your user name and password.

Q: Are there special firewall settings I need to configure for PSP?

A: To enable sFlow and SNMP you'll need to allow outbound bound traffic back to the PSP Data Center subnet range on tcp port 443. Depending on your firewall implementation, UDP 161 must be open from the DMZ to your LAN, and UDP 6343 must allow sFlow traffic from your LAN to the DMZ.

Q: What versions of SNMP does PSP Support?

A: PSP supports SNMP v1, v2c, and v3 as defined in the standard RFCs.

Q: Can my data be intercepted and read when it is being transmitted back to the PSP Data Center ?

A: No. Your identifiable data never leaves your network automatically through the PSP Tools. Only statistical packet information & management data are sent to the PSP Data Center.

Q: What versions of NetFlow and sFlow does PSP Support?

A: PSP supports NetFlow v5 and sFlow v4 and v5.

PSP Online Help is contextually available to authenticated users when logged in to PSP and provides the most detailed and immediate information for answering user and technical questions. The help section is updated regularly in response to user feedback and with each iterative product version release.

Telephone and E-mail Support are available at PSP@extremenetworks.com or by calling the Extreme Networks TAC at:

Americas/AsiaPac: (800) 998-2408

EMEA: +31-30-800-5000

Japan: +81-3-5842-4020

FAX: (408) 579-3000 Attn: PSP@extremenetworks.com

Trademarks

Extreme Networks, the Extreme Networks logo, and Summit are registered trademarks of Extreme Networks, Inc. in the US and other countries. Other trademarks are the property of their respective owners.

