Junos Space Service Insight User Guide

Release
17.1R1

Modified: 2017-06-07

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos Space Service Insight User Guide
17.1R1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- JA2500
- Junos Space Virtual Appliance

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

CHAPTER 1

Junos Space Service Insight Overview

Service Insight Overview

Service Insight is an application that helps in accelerating operational analysis and managing the exposure to known issues. Using Service Insight, you can identify devices that are nearing their End Of Life (EOL) and also discover and prevent issues that could occur in your network. The functionality of Service Insight is dependent on the information sent from Service Now. To enable Service Insight, you must add a valid organization in the Service Now application. See the *Adding an Organization to Service Now* section in the *Junos® Space Service Now User Guide*.

Service Insight identifies the devices available for EOL reports and enables you to generate EOL reports that provide detailed device EOL information about EOL devices, such as the number of devices with EOL parts, EOL announce date, number of EOL announce parts, End Of Engineering SW date, number of End Of Engineering SW parts, End Of Engineering HW date, number of End Of Engineering HW parts, End Of Support date, number of End Of Support parts, top-level assembly parts, circuit assembly parts, PSN numbers, and replacement numbers. See "Exposure Analyzer Overview" on page 25.

Service Insight provides Proactive Bug Notifications (PBNs) as a proactive measure to alert you about known issues that can impact the devices in your network. It is an effective means of communicating the information collected while helping one customer fix issues to another customer who could face similar issues in future. Using this information, which was collected when issues were reported to Juniper Networks, Service Insight identifies devices on your network with similar conditions. PBNs associated with devices on your network are matched and displayed on the **Manage PBNs** page. These PBNs keep you aware of the possible impacts and also of ways to fix the issue. PBNs also consist of workarounds that suggest temporary fixes and instructions that you can follow to protect your network. See "Targeted PBNs Overview" on page 23.

Juniper Care Plus (JCare Plus) customers are entitled to receive PBNs that are managed by the Advanced Services (AS) team. Juniper Care customers are entitled to receive only auto PBNs. Auto PBNs are PBNs that are matched automatically by the system. They

are not managed by the AS team. Customers who do not have JCare Plus license are considered as JCare customers.

Service Insight receives updates about EOL and PBN information from JSS. It also enables you to send notifications about these updates to multiple users and manage these notifications. You can define the events that trigger a notification, the filters that further specify the trigger events, and also the actions that you want Service Insight to take after the notification is triggered. See "Notifications Overview" on page 49.

Service Insight uses two timers, one that runs every midnight, and another that runs every hour. The timers initiate the process to fetch EOL data of devices from JSS.

When a large number of devices is added to Service Insight, EOL data is received by Service Insight in batches. The timer that runs every midnight updates the EOL and PBN data by sending requests to JSS and processing the responses that are received from JSS. If the device information in Service Now and Service insight are not synchronized, the midnight timer initiates a synchronization process so that changes made to devices in Service Now are reflected in Service Insight.

Service Insight Dashboard

The Service Insight dashboard displays notifications and graphically illustrates the number of devices per device group and the number of devices not sending device snapshots. You can access the Service Insight dashboard by selecting **Service Insight** from the **Application Switcher.**

The Service Insight dashboard includes:

Service Insight Workspaces

Apart from the Insight Central and Administration workspaces, Service Insight also provides shortcuts to the Devices and Jobs workspaces by including them in the Service Insight navigation tree. Table 3 on page 17 lists the tasks that can be performed using the Service Insight workspaces.

Table 3: Service Insight Workspaces

Workspace Name	Tasks Included
Insight Central	Using the Insight Central workspace, you can perform the following tasks: • View devices for which EOL reports and associated PBNs are available.. • Generate EOL reports. • Identify PBNs that can affect specific devices. • View list of PBNs associated with devices added in the Service Now application. • Flag PBNs to users. • Assign ownership of PBNs. • E-mail PBN details to users. • Delete PBNs.
Administration (Service Now workspace)	Using the Administration workspace you can perform the following tasks: • Add and manage devices. Adding devices enables you to receive EOL and PBN data for those devices. • Manage script bundles and install and uninstall AI-Scripts on devices. • Add and manage device groups. • Add and manage Service Now organizations. • Configure Service Now global settings.

Dashboard Gadgets

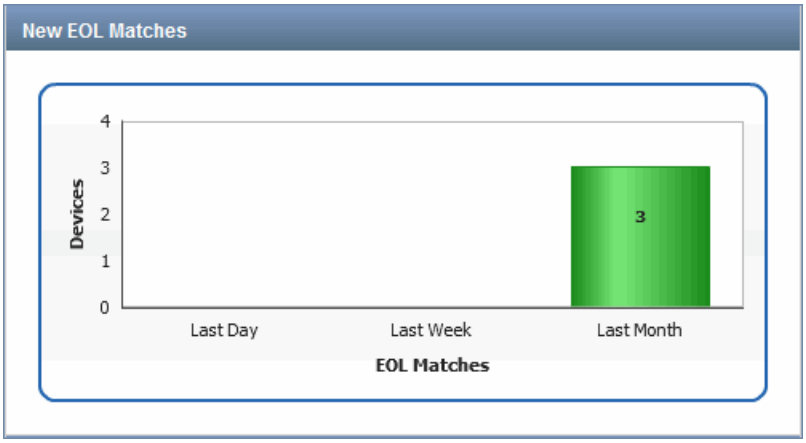
The dashboard displays gadgets with information that is updated automatically and instantaneously. You can move gadgets on the dashboard and change their sizes. These changes persist even after you log back in to the system. The gadgets displayed on the Service Insight dashboard are:

- New EOL Matches on page 17
- Recent PBNs on page 18
- PBN Severity on page 18
- Service Insight Notices on page 19

New EOL Matches

The **New EOL Matches** gadget graphically displays the EOL matches found for the devices on the previous day, the previous week, and the past month. Clicking a bar within the graph takes you to the **Exposure Analyzer** page which displays the devices for which the EOL matches are found.

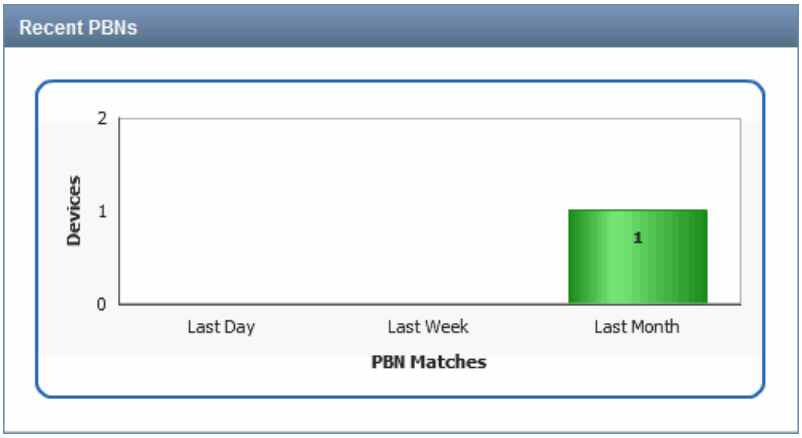
For example, when you click the green bar of the **New EOL Matches** gadget (as shown in the following figure), the **Exposure Analyzer** page displays only the two devices for which EOL notifications were received last month.



Recent PBNs

The **Recent PBNs** gadget graphically displays the devices for which PBNs were received the previous day, the previous week, and the past month. Clicking the bars within the graph takes you to the **Manage PBNs** page which lists the devices for which the PBNs are found.

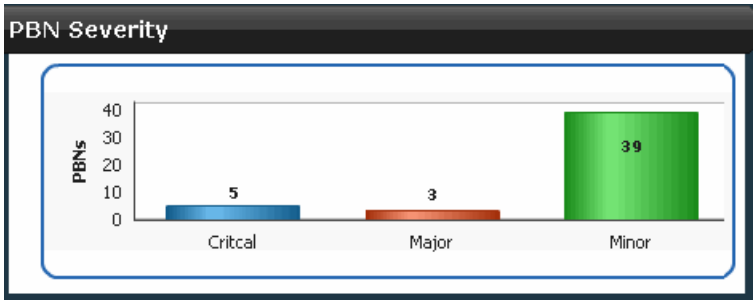
For example, when you click the green bar of the **Recent PBNs** gadget (as shown in the following figure), the **Manage PBNs** page lists only those three devices for which PBNs were received last month.



PBN Severity

The **PBN Severity** gadget graphically displays the severity levels of the received PBNs. Clicking a bar within the graph takes you to the **Manage PBNs** page which lists the PBNs.

For example, when you click the green bar of the **PBN Severity** gadget (as shown in the following figure), the **Manage PBNs** page displays only the PBNs with Minor severity level that were received.



Service Insight Notices

The **Service Insight Notices** gadget provides the following links:

- EOL product information and announcement: http://www.juniper.net/alerts/
- EOS information: https://www.juniper.net/support/eol/

Related Documentation

- Insight Central Overview on page 21
- Service Insight Domain Overview on page 19

Service Insight Domain Overview

A domain is a logical grouping of objects in Junos Space. A Junos Space administrator creates and manages domains in the Junos Space Network Management Platform. For information about domains, see the *Junos Space Network Management Platform User Guide* at Junos Space Network Management Platform Documentation.

When you access Service Insight, only the EOL report, PBN report, and notification objects that are assigned to the domain that you are currently in are visible to you. If you are assigned to more than one domain, you can access those domains and the objects in them by selecting the domains from the **Login as *username* in** list on the banner of the Junos Space GUI. Only the domains to which you are assigned are listed in the **Login as *username* in** list. A super user can access all domains.

EOL report, PBN report, and notification objects that you create when you are logged in to a certain domain are assigned to that domain. If needed, you can assign these objects to another domain. For information about assigning an object to another domain, see "Assigning a Service Insight Object to Another Domain" on page 20.

Targeted PBN objects, used by objects in all domains, are assigned to the system domain. Objects assigned to the system domain are visible on all domains and cannot be assigned to another domain.Table 4 on page 20 lists Service Insight objects and their default domains.

Table 4: Service Insight Objects and Their Default Domains

Service Insight Objects	Default Domain	
	Fresh Installation	Migration
• EOL Reports • PBN Reports • Notifications	Domain to which a user is logged in	Global domain
• Targeted PBNs	System domain	System domain
• Service Insight Devices	Domain assigned to the devices in Junos Space Network Management Platform	Domain assigned to the devices in Junos Space Network Management Platform

Assigning a Service Insight Object to Another Domain

If you are assigned to multiple domains, you can assign a Service Insight object from the domain that you are currently logged in to another domain to which you are assigned. All objects except objects in the system domain can be assigned to another domain.

To assign a Service Insight object to another domain:

1. From the Service Insight navigation tree, select the object.

   The object's page appears.

2. On the object's page, select the object's instance that you want to assign to another domain.

   You can select multiple instances of the object to assign to another domain.

3. From the Actions menu, select **Assign *object* to domain**. Alternatively, right-click the object and select **Assign *object* to domain**.

   The Assign to Domain dialog box appears.

4. Under Assign selected items to domain, select the domain and click **Assign**.

   The Assign to Domain dialog box closes and the object is not listed on the object's inventory landing page.

5. To verify that the object is assigned to the correct domain, from the **Login as *username* in** list, select the domain to which you assigned the object.

   The Service Insight GUI is refreshed.

6. Using the Service Insight navigation tree, open the object's inventory landing page and check whether the object is listed on the page.

Related Documentation

- Insight Central Overview on page 21
- *Administration Overview*
- Domains Overview

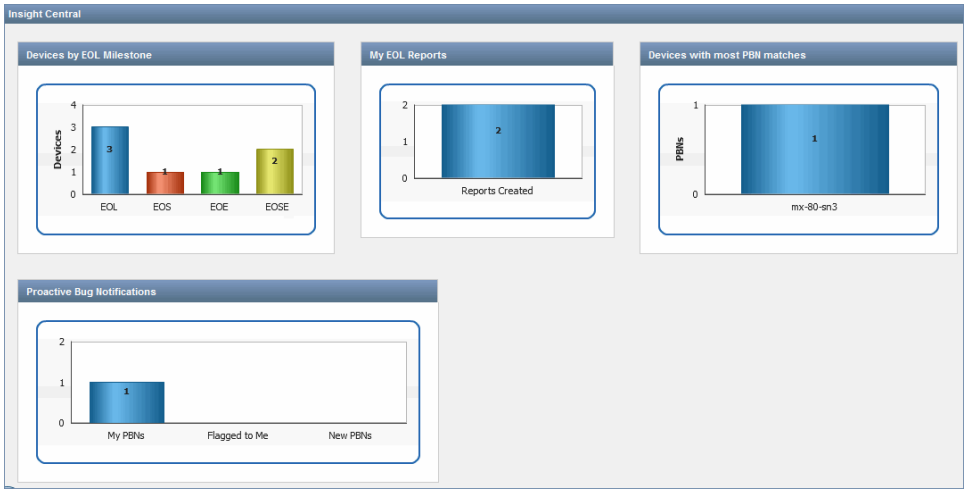
Insight Central Overview

Insight Central is a Service Insight workspace where you can manage devices for which End Of Life (EOL) reports are received, manage the EOL reports and the Proactive Bug Notifications (PBNs). The Exposure Analyzer page within Insight Central displays devices and the available number of EOL parts for these devices, and also displays, for each device, the number of PBNs received. Using the Insight Central workspace, you can also send and manage notifications about EOL and PBN updates to multiple users. You can define the events that trigger a notification, the filters that further specify the trigger events, and also the actions that you want Service Insight to take after the notification is triggered.

To access the Insight Central workspace, you must first enable the Service Insight application. Juniper Care and Juniper Care Plus customers have access to Service Insight. The functionality of Service Insight is dependent on the information sent from Service Now. To enable Service Insight, you must add a valid organization in the Service Now application. See *Adding an Organization to Service Now*.

The Insight Central landing page (as shown in Figure 1 on page 21) graphically displays information about devices and their milestones, EOL reports, PBN reports, the devices with most PBN matches, new PBNs, PBNs owned by you, and the PBNs that are flagged to you.

Figure 1: Insight Central Landing Page



Related Documentation

- Service Insight Overview on page 15
- Exposure Analyzer Overview on page 25

- EOL Reports Overview on page 29
- PBN Reports Overview on page 37
- Targeted PBNs Overview on page 23
- Notifications Overview on page 49

CHAPTER 2

Viewing PBNs and EOL Alerts

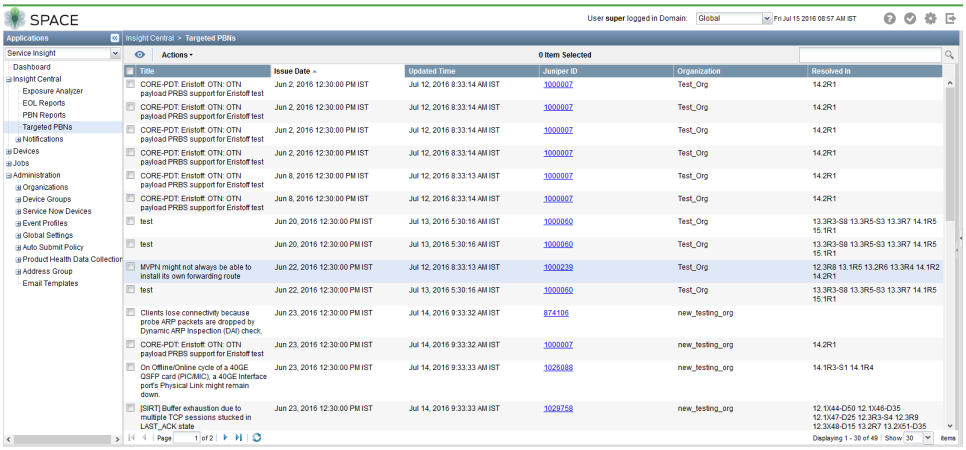
Targeted PBNs Overview

Junos Space Service Insight provides Proactive Bug Notifications (PBNs) as a proactive measure to alert you about known issues that can impact the devices in your network. It is an effective means of communicating information collected while helping one customer fix issues to another customer who could face similar issues in future.

Using this information, which was collected when issues were reported to Juniper Networks, Service Insight identifies devices on your network with similar conditions. When devices are identified on your network to have similar configuration as those devices on which issues were found, PBNs associated with these devices are displayed on the **Targeted PBNs** page. These PBNs keep you aware of the possible impacts and also of ways to fix the issue. PBNs also contain workarounds that suggest temporary fixes and instructions that you can follow to protect your network. Service Insight checks for new PBNs and updates the existing PBNs every 24 hours.

In Service Insight, targeted PBNs are listed on the Targeted PBNs page (Service Insight > Targeted PBNs) as shown in Figure 2 on page 24.

Figure 2: Targeted PBNs Page



A targeted PBN contains the fields listed in Table 5 on page 24. On the targeted PBNs page, you can filter and view PBNs based on organization. Using a targeted PBN, you can scan for devices impacted by the vulnerabilities described in the targeted PBN in an organization and list the devices; for more information, see "Scanning PBNs for Impact on Devices" on page 38.,

Table 5: Targeted PBNs Field Descriptions

Field	Description
Title	Short description of the issue found
Issue Date	Date and time when the issue was recorded
Updated Time	Date and time the PBN was last updated
Juniper ID	Unique ID specified by Juniper Networks that is used to identify the PBN
Organization	Organization to which the PBN is applicable
Resolved In	Date and time when the problem in this PBN was resolved
Description	Short description of the problem
Trigger	Conditions that initiated the problem described by the PBN
Symptom	Conditions that indicate that the problem described by the PBN has occurred
Work Around	Temporary fix for the problem
Instructions	Additional information that you can follow
Relevances	The platforms and device that could be impacted by the problem described by the PBN

Table 5: Targeted PBNs Field Descriptions *(continued)*

Field	Description
Customer Impact	The impact of the bug on the customer network
Impact Probability	The probability that the bug would impact the network
Owner	The user who has been assigned ownership of the PBN using Service Insight
Flagged to Users	The users who were notified about the PBN using Service Insight

You can perform the following tasks using the Targeted PBNs page:

- Scan for devices that are impacted by PBNs; see "Scanning PBNs for Impact on Devices" on page 38 for details.
- Flag PBNs to users; see "Flagging PBNs to Users" on page 39 for details.
- E-mail PBNs to users; see "E-Mailing PBNs" on page 41 for details.
- Assign an owner to a PBN; see "Assigning an Owner to a PBN" on page 39 for details.
- Delete one or more PBNs; see "Deleting PBNs" on page 40 for details.

Related Documentation

- Exposure Analyzer Overview on page 25

Exposure Analyzer Overview

Service Insight lists devices and any End of Life (EOL) reports or Proactive Bug Notifications (PBNs) that are received for the devices(see Figure 3 on page 26). The Quick View area of Exposure Analyzer page displays the devices (showing details such as number of EOL parts and number of matching PBNs) with specific icons. Table 6 on page 26 describes these icons. Table 7 on page 26 describes the fields on the Exposure Analyzer page and the Device Details page.

Using Exposure Analyzer, you can generate EOL reports and PBN reports for a particular device. The reports are exported in Excel format. An EOL report includes the following items: devices with End of Life announce parts, serial number of the device, model number of the device, top level assembly part for the device, End of Sale date, and End of Service date, Last Hardware Engineering Support date, Last Software Engineering Support date for the devices that you select. A PBN report includes the following items: Device Name, Device Serial Number, Product, Junos Version, Device Group, Connected Member, Organization, PBN Title, Juniper ID, PBN Description, PBN Customer Impact, PBN Work Around, and PBN URL. EOL reports and PBN reports are exported in Excel format.

Service Insight uses two timers, one that runs every midnight, and another that runs every hour. The hourly timer initiates the processing of pending EOL requests. This timer schedules when JSS sends these requests to the corresponding devices. When large number of devices are added to Service Insight, JSS sends these requests in batches. The timer that runs every midnight updates the EOL and PBN data by sending requests

to JSS and processing the responses that are received from JSS. This timer also initiates the synchronization process between Service Now and Service Insight which enables Service Insight to display the changes that were made to devices in Service Now. When you execute device related actions in Service Now while either one of these timers is running, Service Insight takes an hour to display the changes corresponding to these actions on the **Exposure Analyzer** page.

Figure 3: Exposure Analyzer Page

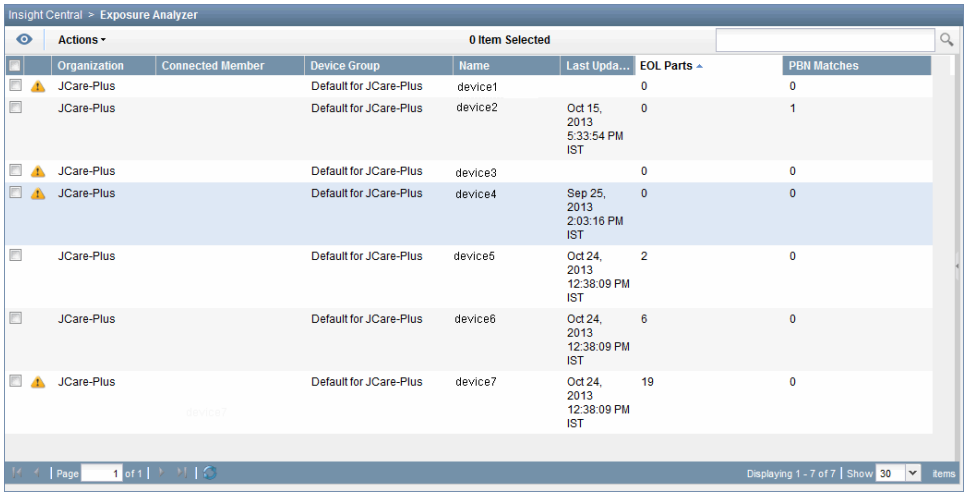


Table 6 on page 26 describes the icons on the exposure analyzer page.

Table 6: Exposure Analyzer Page Icon Descriptions

Icon	Description
	An EOL report is received for the device
	A PBN Is received for the device.

Table 7 on page 26 describes the fields on the Exposure Analyzer page and the Device Details dialog box.

Table 7: Device Details from the Exposure Analyzer Page

Field	Description
Name	The device hostname.
Serial Number	Serial number of the device chassis.
IP Address	IP address of the device.
Product	Model number of the device.
Organization	Service Now organization to which the device belongs.

Table 7: Device Details from the Exposure Analyzer Page *(continued)*

Field	Description
Device Group	Service Now device group to which the device belongs.
Connected Member	Customer connected to the device.
Connection Status	Connection status of the device in Junos Space. • up—device is connected to Junos Space. • down—device is not connected to Junos Space.
EOL status	EOL information of the device.
EOL Parts	The parts of the device identified for EOL.
Matching PBNs	Number of PBNs received for the device.
Last updated	Latest date and time when the device connection was updated.

You can perform the following tasks from the **Exposure Analyzer** page:

- Generate EOL reports; see "Generating EOL Reports" on page 34 for details.
- Generate PBN reports; see "Generating PBN Reports" on page 41 for details.
- View PBNs that are applicable to devices in your network; see "Showing Matching PBNs" on page 27 for detials.

Related Documentation

- Targeted PBNs Overview on page 23
- Notifications Overview on page 49

Showing Matching PBNs

Using Service Insight, you can view the list of PBNs that are associated with one device or up to ten devices simultaneously.

To view PBNs for a device:

1. From the Service Insight navigation tree, select **Insight Central** > **Exposure Analyzer**. The list of devices appears.
2. Select the devices for which PBNs are to be viewed. You can select up to ten devices.
3. Right-click your selection or use the **Actions** list and select **Show Matching PBNs**. The **Manage PNBs** page displays the list of PBNs that are associated with the device that you selected.

Related Documentation

- Exposure Analyzer Overview on page 25
- Targeted PBNs Overview on page 23
- Notifications Overview on page 49

CHAPTER 3

Managing EOL Alerts

EOL Reports Overview

The **EOL Reports** page displays the End of Life (EOL) reports that you generate as shown in Figure 4 on page 29. Using this page, you can export the existing EOL reports to an Excel file, regenerate the report to get the latest information, and delete the EOL reports from the Service Insight database. To filter the devices that have EOL parts, double-click an EOL report to display its detailed summary view, and click the number in the **Devices Selected** field.

Figure 4: EOL Reports Page View

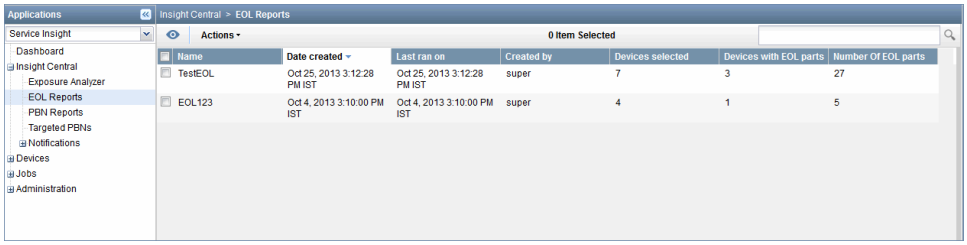


Table 8 on page 29 describes the fields on the **EOL Reports** page and the **EOL Report Detail** dialog box.

Table 8: EOL Reports Page and EOL Report Detail Dialog Box Fields Description

Field	Description
Name	Name of the EOL report.
Date created	Date and time when the EOL report was created.
Last Ran On	Date and time when the EOL report was last regenerated.

Table 8: EOL Reports Page and EOL Report Detail Dialog Box Fields Description *(continued)*

Field	Description
Created by	Name of the user who created the EOL report.
Devices selected	Number of devices that were selected to generate the EOL report. Clicking the number takes you to the **Exposure Analyzer** page which displays only the devices with EOL parts.
Devices with EOL parts	Number of devices with parts for which end-of-life is announced or is in the process of being announced. The EOL date of a part specifies the date when Juniper Networks announced the end-of-life of the part.
End of Life Announce parts	Number of parts in the devices in the EOL report for which EOL dates are announced.
End of Sale parts	Number of parts in the devices in the EOL report for which the end of sale date has exceeded. Juniper Networks or a Juniper Networks partner do not sell these parts after the end of sale date. The end of sale date of a part specifies the last day to buy a product, order a new service contract, or add the part to an existing support contract. After the end of sale date, parts and services are removed from price lists.
Last Hardware Engineering Support parts	Number of parts in the devices in the EOL report for which hardware is no longer available for order or RMA. The last hardware engineering support date for a part specifies the last day the hardware engineering in Juniper Networks will support the part.
Last Software Engineering Support parts	Number of parts in the devices in the EOL report for which software or firmware is no longer available from Juniper Networks. The last software engineering support date of a part specifies the last date till which new (that is, non-maintenance) software releases will support the product. After this date, new software releases will not support the product. Maintenance releases of the major software releases issued prior to this date will support the product within the current software EOL guidelines.
End of Service parts	Number of parts in the devices in the EOL report for which end of service date is exceeded. The end of service date of a part specifies the last date to receive contracted service (including hardware and software bug fixes, and logistics replacement or repair services) for the part.

You can perform the following tasks using the **EOL Reports** page:

- Export EOL reports; see "Exporting EOL Reports" on page 33 for details.
- Regenerate EOL reports; see "Regenerating EOL Reports" on page 31 for details.
- Delete EOL reports; see "Deleting EOL Reports" on page 31 for details.

Related Documentation

Generating EOL Reports on page 34

Deleting EOL Reports

You can delete multiple EOL reports from the EOL Reports page. Deleted EOL reports cannot be recovered.

To delete EOL reports:

1. From the Service Insight navigation tree, select **Insight Central** > **EOL Reports**.
   The EOL reports are displayed.
2. Select one or more EOL reports that you want to delete.
3. Select **Delete** either from the **Actions** list or the right-click menu.
   The **Delete EOL Reports** dialog box appears and displays the names of the selected EOL reports.
4. Click **Delete**.
   The selected EOL reports are deleted from the database and are no longer displayed on the **EOL Reports** page.

Related Documentation

- Generating EOL Reports on page 34
- EOL Reports Overview on page 29

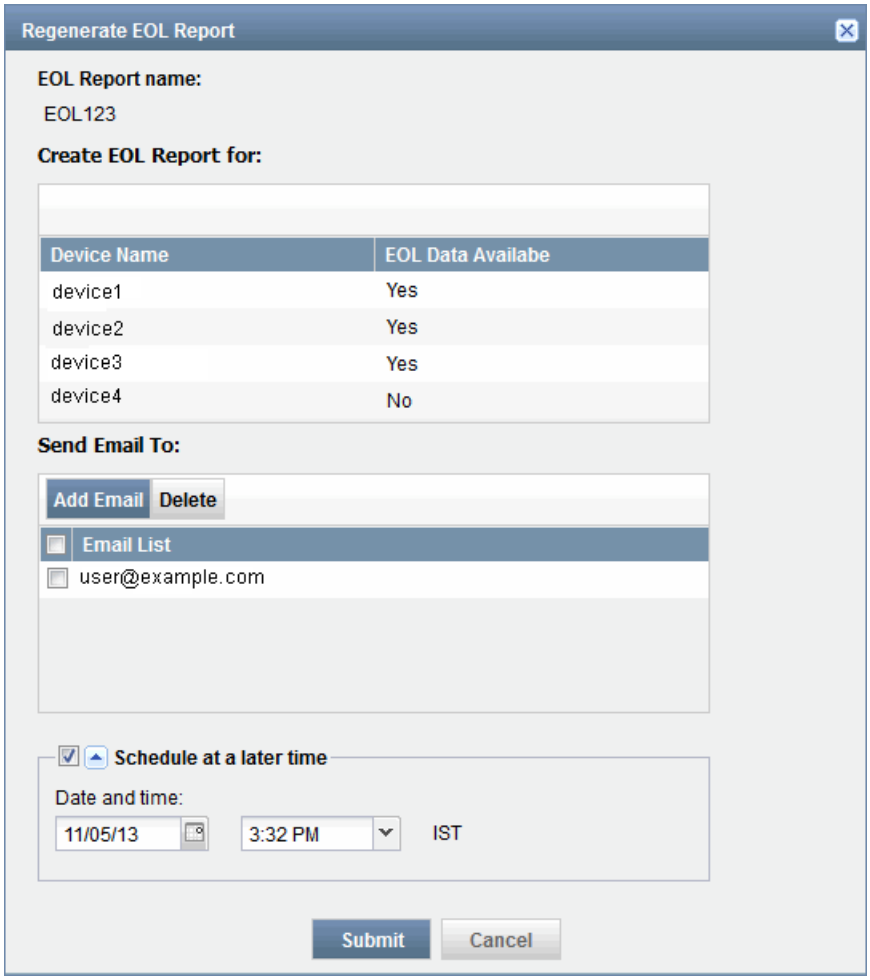
Regenerating EOL Reports

Using Service Insight, you can regenerate an EOL report to get the latest EOL information.

To regenerate EOL reports:

1. From the Service Insight navigation tree, select **Insight Central** > **EOL Reports**.
   The EOL Reports page is displayed.
2. Select the EOL report that you want to regenerate.
3. Select **Regenerate EOL Reports** from either the **Actions** list or the right-click menu.
   The **Regenerate EOL Report** dialog box displays the name of the EOL report, the device name with which the EOL report is associated, and the e-mail addresses specified.
   See Figure 5 on page 32.

Figure 5: Regenerate EOL Report Dialog Box



4. (Optional) To modify the list of e-mail addresses of users to whom the EOL report must be sent, use the **Add Email** and **Delete** buttons.

5. (Optional) To schedule a time for regenerating the report, select the **Schedule at a later time** check box and specify the date and time when you want the EOL report to be regenerated.

6. Click **Submit**.
   The Job Information dialog box displays a Job ID link. Click this link to view the status of this action on the **Jobs** page.

Related Documentation

- EOL Reports Overview on page 29
- Generating EOL Reports on page 34
- Exporting EOL Reports on page 33

Exporting EOL Reports

You can export the information in an EOL report to an Excel file and save it on your local file system. The EOL report includes the following information:

- Product: The device with parts for which EOL is announced
- Serial#: Serial number of the device chassis. with parts for which EOL is announced
- Device: The host name of the device
- PSN#: The product specification notification for the part
- EOL Model#: The model number of the part for which EOL is announced
- Top Level Assembly#: The top level assembly part number of the part for which EOL is announced
- Circuit Assembly Part#: The circuit assembly part number of the part for which EOL is announced
- EOL Announce Date: The date when Juniper Networks announced the end of life of a product
- Announcement Type: Indicates if the device component is end of sale, end of life, or if the component is RoHS compliant and available restrictedly.
- End of Sale Date: Specifies the last day to buy a product, order a new service contract, or add the part to an existing support contract.

  After the end of sale date, parts and services are removed from price lists.
- Last Software Engineering Date: Specifies the last date till which new (that is, non-maintenance) software releases will support the product

  After this date, new software releases will not support the product. Maintenance releases of the major software releases issued prior to this date will support the product within the current software EOL guidelines.
- Last Hardware Engineering Date: Specifies the last day the hardware engineering in Juniper Networks will support the part
- End of Service Date: Specifies the last date to receive contracted service (including hardware and software bug fixes, and logistics replacement or repair services) for the part
- Replacement#: The model number of the part with which the EOL part existing in the device can be replaced
- Quantity: The number of units to be replaced
- Replacement Model Description: The description of the component that can replace the outdated part in the product
- RoHS Compliance: Indicates if the part is RoHS compliant or not

To export EOL reports:

1. From the Service Insight navigation tree, select **Insight Central** > **EOL Reports**. The **EOL Reports** page appears.
2. Select the report that you want to export to the Excel file.
3. Select **Export EOL Reports** from either the **Actions** list or the righ-click menu. The **Export EOL Report** appears.
4. Click the **Click here to download EOL reports** link and save the file to your local file system.

Related Documentation

- EOL Reports Overview on page 29
- Generating EOL Reports on page 34
- Regenerating EOL Reports on page 31
- Deleting EOL Reports on page 31

Generating EOL Reports

Devices with End of Life (EOL) information are identified and displayed on the Exposure Analyzer page. Using Service Insight, you can generate EOL reports for these devices in an Excel file. EOL reports provide information such as the number of devices with EOL parts, EOL announce date, number of EOL announce parts, Last Software Engineering Support date, number of Last Software Engineering Support parts, Last Hardware Engineering Support date, number of Last Hardware Engineering Support parts, End of Sale date, End of Service date, top-level assembly parts, circuit assembly parts, PSN numbers, and replacement numbers. You can also schedule a time for generating the EOL reports.

To generate EOL reports:

1. From the Service Insight navigation tree, select **Insight Central** > **Exposure Analyzer**. The list of devices appears.
2. Select one or more devices for which you want to generate the EOL report.
3. Select **Generate EOL Reports** either from the **Actions** list or the right-click menu. The **Generate EOL Report** dialog box appears.
4. (Optional) Select the **Do not save this report on Service Insight** check box if you do not want to save the EOL report. By default, the check box is clear and PBN reports are stored in the Service Insight database.

5. Enter a name for the EOL report.

   The name can contain alphanumeric characters (a–z, A–Z, 0–9), space, underscore (_), and hyphen (-).

6. For the **Create EOL Report for** option, select one of the following:

   - To generate EOL report for a particular organization or device group,

     a. Click **All devices**.

        Organization and Device groups drop down menu are displayed.

     b. From the **Organization** or **Device Group** drop down menu, select the organization or device group for which you want to generate the EOL report.

   - To generate EOL report for devices selected in step 2, click **Selected devices shown below**.

7. Enter the e-mail address of the user to whom the EOL report must be sent.

   To add and delete users who must receive the e-mail, use the **Add Email** and **Delete** buttons. By default, the **Send Email To** list contains the e-mail address of the logged-in user.

8. To schedule a time for generating the report, select the **Schedule at a later time** check box and set the date and time for the EOL report to be generated.

9. Select **Repeat** and schedule an interval for regenerating the EOL report.

   The report generated for the first time has the name given by the user and for all the other successive reports, the report name is appended with timestamp.

10. Click **Submit**.
    The Job Information dialog box displays a job ID link for the generated report.

11. Click the job ID link.

    The Jobs page displays the details of the generated EOL report. The report includes the schedule for the generation of successive PBN reports if the Repeat option is configured.

12. If you want to cancel the scheduled job for generating the next EOL report, select **Cancel Job** either from the **Actions** list or the right-click menu.

Related Documentation

- EOL Reports Overview on page 29
- Generating EOL Reports on page 34
- Regenerating EOL Reports on page 31

- Deleting EOL Reports on page 31

CHAPTER 4

Managing PBN Alerts

PBN Reports Overview

The **PBN Reports** page displays the PBN reports that you generate as shown in Figure . Using this page, you can export the existing PBN reports to an Excel file, regenerate them to get the latest information, and delete them from the Service Insight database. To filter the devices that have PBN data, double-click a PBN report to display its detailed summary view, and click the link at the bottom of the displayed dialog box. See Figure 6 on page 37.

Figure 6: PBN Reports page

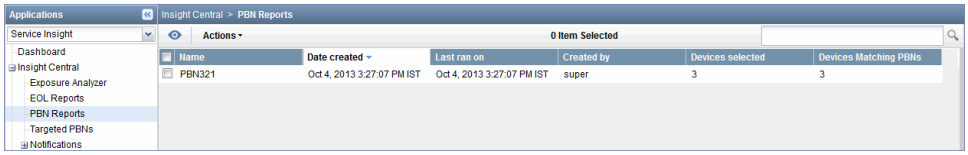


Table 9 on page 37 describes the fields on the Manage PBN Reports page and the PBN Report Detail dialog box.

Table 9: PBN Reports Page and PBN Report Detail Dialog Box Fields Description

Field	Description
Name	Name of the PBN report.
Date Created	Date and time when the PBN report was created.

Table 9: PBN Reports Page and PBN Report Detail Dialog Box Fields Description *(continued)*

Field	Description
Last Ran On	Date and time when the PBN report was last run.
Created By	Name of the user who created the PBN report.
Devices Selected	Number of devices that were selected to generate the PBN report.
Device Name	Name of the device.
Devices with PBNs	Number of devices for which PBNs have been received.

You can perform the following tasks using the **PBN Reports** page:

- Export PBN reports; see "Exporting PBN Reports" on page 46 for details..
- Regenerate PBN reports; see "Regenerating PBN Reports" on page 44 for details.
- Delete PBN reports; see "Deleting PBN Reports" on page 47 for details.

Related Documentation

- Generating PBN Reports on page 41

Scanning PBNs for Impact on Devices

You can use Service Insight to identify the devices within an organization that could be impacted by the vulnerabilities described in a targeted PBN.

To scan PBNs and view the impacted devices:

1. From the **Service Insight** taskbar, select **Insight Central > Targeted PBNs**.

   The Targeted PBNs page displays the list of PBNs.

2. Select the PBN that you want to scan for impact.

3. Right-click your selection or use the **Actions** list and click **Scan for Impact**.

   The **Scan for Impact** dialog box lists the PBNs selected to determine the devices that are impacted.

4. Click **Confirm** to scan the PBNs.

   The Job Information page displays the schedule status of the selected PBNs. To view the details, click the Job ID. The scan details appear on the Job Management page.

Related Documentation

- Exposure Analyzer Overview on page 25
- Assigning an Owner to a PBN on page 39

Flagging PBNs to Users

You can flag PBNs to Junos Space users who you think need to keep track of the PBNs or who need to receive them.

To flag PBNs to a user:

1. From the **Service Insight** navigation tree, select **Insight Central > Targeted PBNs**.

   The **Manage PBNs** page displays the list of PBNs.

2. Select one or more PBNs that you want to flag to the user.

3. From the Actions list or the right-click menu, select **Flag to Users**.

   The Flag to Users dialog box displays the list of users who have permissions to view, assign ownership, or delete PBNs.

4. Select the users to whom the PBN must be flagged.

5. Select the **Email PBN to Flagged Users** check box to send an e-mail notification to all the newly flagged users. This option is selected by default.

6. Click **Submit**.

   The specified users receive notification about the selected PBN.

To verify that the specified users have been notified of the selected PBN, double-click the PBN and view the **Flagged to Users** field of the PBN in the **PBN. Details** dialog box.

Related Documentation

- Assigning an Owner to a PBN on page 39
- E-Mailing PBNs on page 41
- Deleting PBNs on page 40

Assigning an Owner to a PBN

You can assign a PBN to a Junos Space user who needs to be notified of the PBN and is responsible for the PBN.

To assign ownership of a PBN:

1. From the Service Insight navigation tree, select **Insight Central** > **Targeted PBNs**.
   The **Manage PBNs** page displays the list of PBNs.

2. Select the PBN to which you want to assign an owner.

3. Right-click your selection or use the **Actions** list, select **Assign Ownership**.
   The Assign Ownership dialog box appears

4. Enter the login ID of the user who would own the selected PBN.

5. Select the **Email PBN to Assigned Owner** check box to send an e-mail notification to the assigned owner. This option is selected by default.

6. Click **Submit**.
   The selected PBN is assigned to the specified user.
   To verify that the selected PBN is assigned to the specified user, double-click the PBN on the **Targeted PBNs** page and view the **Owner** field of the PBN in the **PBN Details** dialog box.

Related Documentation

- Exposure Analyzer Overview on page 25
- Scanning PBNs for Impact on Devices on page 38
- E-Mailing PBNs on page 41
- Flagging PBNs to Users on page 39

Deleting PBNs

You can delete PBNs that are displayed on the Manage PBNs page.

To delete PBNs:

1. From the Service Insight navigation tree, select **Insight Central** > **Targeted PBNs**.
   The Manage PBNs page displays the list of PBNs.

2. Select the PBNs that you want to delete.

3. Right-click your selection or use the **Actions** list and select **Delete**.
   The **Delete PBNs** dialog box displays a list of the selected PBNs.

4. Click **Delete** to confirm.
   The selected PBNs are deleted from the Service Insight database and no longer listed in the Targeted PBNs page.

Related Documentation

- Exposure Analyzer Overview on page 25
- Scanning PBNs for Impact on Devices on page 38
- Assigning an Owner to a PBN on page 39
- Generating PBN Reports on page 41

E-Mailing PBNs

Using Junos Space, you can e-mail PBN details to multiple users.

To e-mail PBN details:

1. From the Service Insight navigation tree, select **Insight Central** > **Targeted PBNs**.
   The **Manage PBNs** page displays the list of PBNs.
2. Select the PBN that you want to e-mail to users.
3. Right-click your selection or use the **Actions** list and select **Email**.
   The **Email PBN Details** dialog box appears.
4. Use the **Add Email** and **Delete** buttons to add and delete e-mail IDs of users to whom the selected PBN details need to be sent. By default, the e-mail ID of the logged-in user is added to the **Send Email To** list of users.
5. (Optional) To schedule a time for e-mailing the selected PBNs, select the **Schedule at a later time** check box and specify the date and time when you want the PBNs to be e-mailed.
6. Click **Submit**.
   The selected PBNs are e-mailed to the specified users.

Related Documentation

- Assigning an Owner to a PBN on page 39
- Flagging PBNs to Users on page 39
- Scanning PBNs for Impact on Devices on page 38

Generating PBN Reports

Service Insight provides Proactive Bug Notifications (PBNs) as a proactive measure to alert about known issues that can impact the devices in the network. You can also set the scheduling time for generating PBN reports such that they are generated on a set schedule. Devices with PBN information are identified and displayed on the Exposure Analyzer page. Using Service Insight, you can generate PBN reports for these devices in an Excel file. A PBN report includes the following items: Device Name, Device Serial Number, Product, Junos Version, Device Group, Connected Member, Organization, PBN Title, Juniper ID, PBN Description, PBN Customer Impact, PBN Work Around, and PBN URL.

To generate PBN reports:

1. From the Service Insight navigation tree, select **Insight Central** > **Exposure Analyzer**.

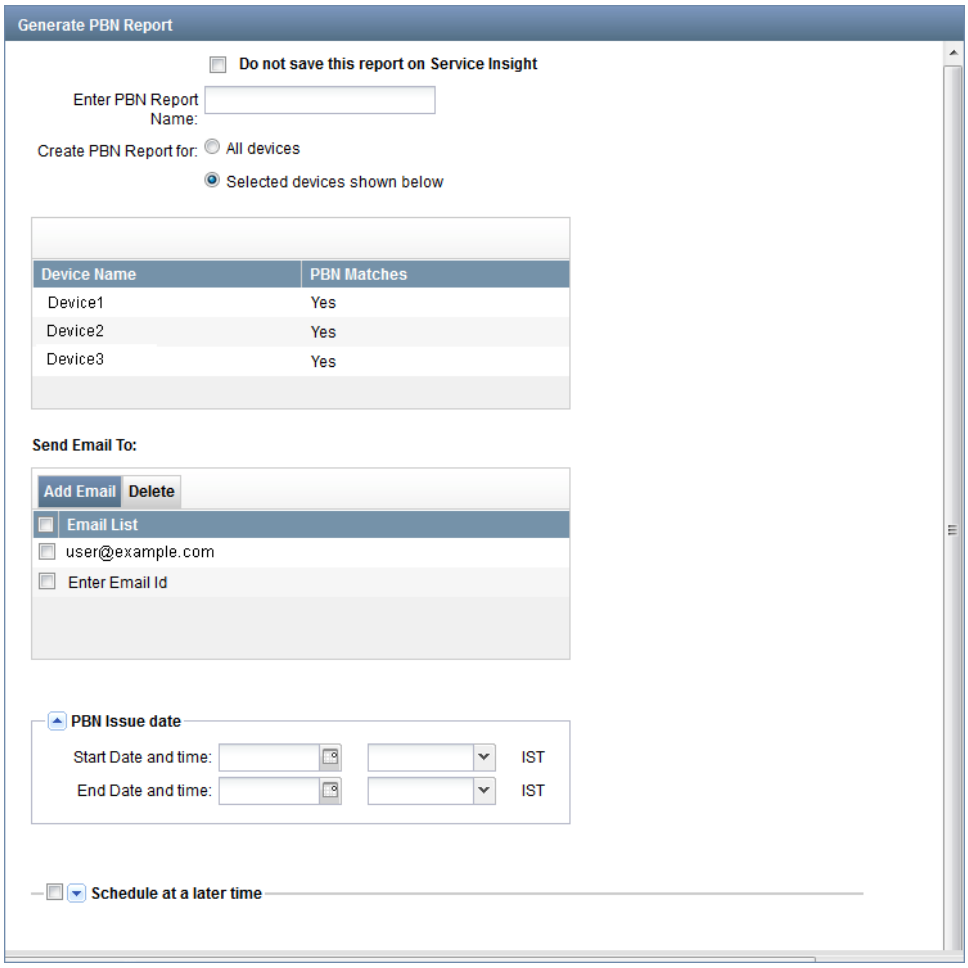
   The list of devices appears.

2. Select one or more devices for which you want to generate the PBN report.

3. From the **Actions** menu, select **Generate PBN Reports**. Alternatively, right-click and select **Generate PBN Reports**.

   The **Generate PBN Report** dialog box appears as shown in Figure 7 on page 42.

Figure 7: Generate PBN Report Dialog Box



4. (Optional) Select the **Do not save this report on Service Insight** check box if you do not want to save the PBN report. By default, the check box is clear and PBN reports are stored in the Service Insight database.

5. In the **Enter PBN Report Name** text box, enter a name for the PBN report.

The name can contain alphanumeric characters (a–z, A–Z, 0–9), space, underscore (_), and hyphen (-).

6. For the **Create PBN Report for** option, select one of the following:
   - To generate EOL report for a particular organization or device group,
     a. Click **All devices**.

        Organization and Device groups drop down menu are displayed.

     b. From the **Organization** or **Device Group** drop down menu, select the organization or device group for which you want to generate the EOL report.
   - To generate EOL report for devices selected in step 2, click **Selected devices shown below**.
7. For the **Send Email To:** option, enter the e-mail address of the user to whom the PBN report must be sent.

   To add and delete users who must receive the e-mail, use the **Add Email** and **Delete** buttons, respectively. By default, the **Send Email To** list contains the e-mail address of the logged-in user.
8. (Optional) Under the **PBN issue date** option, select values for **Start Data and time** and **End Date and time** to generate a report of the devices affected by PBNs issued during the selected time period.

   NOTE:

   - If a Start Date and time and End Date and time are not specified, managed devices in your network affected by all the PBNs issued by Juniper Support System (JSS) since the inception of JSS are reported.
   - If you select only the start date and time, the devices in your network affected by all the PBNs issued from the selected Start Date and time till you generate the report are included in the report.
   - If you select only the End Date and time, the devices in your network affected by all the PBNs issued by JSS since its inception and till the selected end date and time are included in the report.
9. (Optional) To schedule a time for generating the report, select the **Schedule at a later time** check box and set the date and time for the PBN report to be generated.
10. Select **Repeat** and schedule an interval for regenerating the PBN report.

    The report generated for the first time has the name you provide. All successive reports have the date and time the report is generated appended to the name that you provide.

11. Click **Submit** after selecting the required options.

    The Job Information dialog box displays a *job ID* link for the generated report.

    If you have selected the **Do not save this report on Service Insight** check box, a **Download** link is provided to download the PBN report as an Excel file; otherwise, the PBN report is stored on Service Insight and can be viewed on the PBN Reports page (**Insight Central > PBN Reports**) after the job is completed.

12. Click the *job ID* link.

    The Jobs page displays the details of the generated PBN report. The report includes the schedule for the generation of successive PBN reports if the Repeat option is configured.

    The generated report can be saved or downloaded as an Excel sheet. The saved report can be viewed in PBN reports page.

13. If you want to cancel the job scheduled for generating the next PBN report, select **Cancel Job** either from the **Actions** list or the right-click menu.

Related Documentation

- PBN Reports Overview on page 37
- Regenerating PBN Reports on page 44
- Exporting PBN Reports on page 46
- Deleting PBN Reports on page 47

Regenerating PBN Reports

Junos Space Service Insight provides the *Regenerate PBN Reports* option on the Actions menu to regenerate reports on proactive bug notifications (PBNs) to get information about devices impacted by latest PBNs issued by Juniper Support System (JSS).

To regenerate PBN reports:

1. From the Service Insight navigation tree, select **Insight Central** > **PBN Reports**.

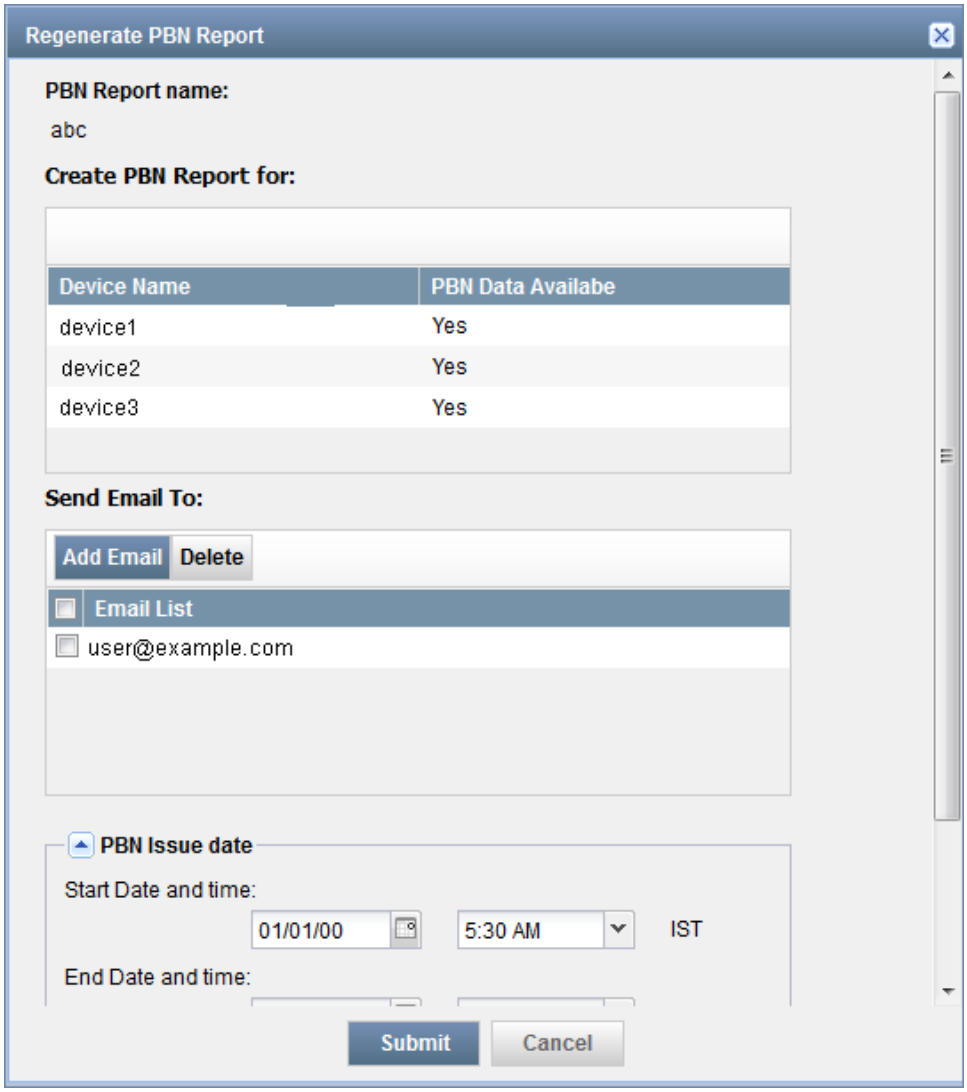
   The PBN reports are displayed.

2. Select the PBN report that you want to regenerate.

3. From the **Actions** menu, select **Regenerate PBN Reports**. Alternatively, right-click the PBN report and select **Regenerate PBN Reports**.

   The **Regenerate PBN Report** dialog box displays the name of the PBN report, the device name with which the PBN report is associated, and the e-mail addresses specified. See Figure 8 on page 45 .

Figure 8: Regenerate PBN Report Dialog Box



4. (Optional) To add or delete users who must receive the e-mail, use the **Add Email** and **Delete** buttons respectively.

5. (Optional) Under the **PBN issue date** option, select values for **Start Data and time** and **End Date and time** to generate a report of the devices affected by PBNs issued during the selected time period.

NOTE:

- If a Start Date and time and End Date and time are not specified, managed devices in your network affected by all the PBNs issued by Juniper Support System (JSS) since the inception of JSS are reported.
- If you select only the start date and time, the devices in your network affected by all the PBNs issued from the selected Start Date and time till you generate the report are included in the report.
- If you select only the End Date and time, the devices in your network affected by all the PBNs issued by JSS since its inception and till the selected end date and time are included in the report.

6. (Optional) To schedule a time for regenerating the report, select the **Schedule at a later time** check box and specify the date and time when you want the PBN report to be regenerated.

7. Click **Submit**.
   The Job Information dialog box displays a *Job ID* link. Click this link to view the status of the job on the **Manage Jobs** page.

Related Documentation

- PBN Reports Overview on page 37
- Exporting PBN Reports on page 46
- Generating PBN Reports on page 41
- Deleting PBN Reports on page 47

Exporting PBN Reports

You can export the information in a PBN report to an Excel file and save it on your local file system. The PBN report includes information such as the Device Name, Device Serial Number, Product, Junos Version, Device Group, Connected Member, Organization, PBN Title, Juniper ID, PBN Description, PBN Customer Impact, PBN Work Around, PBN URL.

To export PBN reports:

1. From the Service Insight navigation tree, select **Insight Central** > **PBN Reports**.
   The **PBN Reports** page appears.

2. Select the report that you want to export to an Excel file.

3. Select **Export PBN Reports** from either the **Actions** list or the right-click menu.

The **Export PBN Report** dialog box appears.

4. Click the **Click here to download PBN reports** link and save the file to your local file system.

Related Documentation

- PBN Reports Overview on page 37
- Generating PBN Reports on page 41
- Regenerating PBN Reports on page 44
- Deleting PBN Reports on page 47

Deleting PBN Reports

You can delete multiple PBN reports from the PBN Reports page. Deleted PBN reports cannot be recovered.

To delete PBN reports:

1. From the Service Insight navigation tree, select **Insight Central** > **PBN Reports**.
   The PBN reports are displayed.
2. Select one or more PBN reports that you want to delete.
3. Select **Delete** from the Action list or the right-click menu.
   The **Delete PBN Reports** dialog box displays the names of the selected PBN reports.
4. Click **Delete**.
   The selected PBN reports are deleted from the database and are no longer displayed on the **PBN Reports** page.

Related Documentation

- Generating PBN Reports on page 41
- PBN Reports Overview on page 37

CHAPTER 5

Service Insight Notifications

Notifications Overview

In Service Insight, you can create notifications to alert users when a specific event occurs. You can also specify the actions that Service Insight must take when an event is triggered.

Specify the following parameters when you create a notification:

- Trigger—Specify the event that causes Service Insight to send the notification. The types of triggers are:
  - New EOL Match—an e-mail notification is sent when an EOL announcement is received and one or more devices are affected by the announcement.
  - New PBN Arrival—an e-mail notification is sent when a new PBN is received and matches one or more devices.
  - New PBN Match—an e-mail notification is sent when a PBN affects one or more devices.
- Filters—Specify additional details about the event that cause Service Insight to send a notification.
- Actions—Specify the action (or actions) that must be taken after a specified event is triggered. These events can be filtered by public tags (applied on devices listed on the Exposure Analyzer page), device name, and serial number.

The Notifications page enables you to manage these notifications. This page displays the notifications chronologically by name, owner, status, and trigger. Table 10 on page 50 provides more information about the fields on the **Manage Notifications** page.

Table 10: Manage Notifications Page Fields Description

Field Name	Description	Range/Length
Name	Name of the notification.The notification name must be unique	64 characters
Owner	User name of the user who owns the notification.	Not applicable
Status	Functional status of the notification.	Enabled or Disabled
Trigger Type	Type of the trigger for which the notification is applied.	• New EOL Match • New PBN Arrival • New PBN Match

On the Service Insight Notifications page, you can perform the following tasks:

- Create and copy notifications; see "Creating and Copying a Notification" on page 50 for details.
- Edit filters and actions of a notification; see "Editing the Filters and Actions of a Notification" on page 53 for details.
- Enable or disable notifications; see "Enabling and Disabling Notifications" on page 53 for details.
- Delete notifications; see "Deleting Notifications" on page 54 for details.

Related Documentation

- Targeted PBNs Overview on page 23

Creating and Copying a Notification

You can specify when you want Service Insight to send notifications, and also the recipients of the notification. You can define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Insight to take after the event is triggered. Service Insight enables you to create and copy notifications:

- Creating a Notification on page 51
- Copying a Notification on page 51

Creating a Notification

To create a notification policy:

1. From the Service Insight navigation tree, select **Insight Central** > **Notifications** > **Create Notifications**.
   The **Create Notifications** dialog box appears. For descriptions about the fields on this page see Table 11 on page 52.

2. Enter a name for the notification and select a trigger.

3. (Optional) Specify filters, such as the tags included, device name, and serial number. When you select the **New PBN Arrival** or **New PBN Match** trigger, you are allowed to specify two additional filters. These two filters allow you to filter the PBNs based on the words that it has or does not have.

4. Enter the e-mail IDs of the recipients of the notification using the **Add Email** button.

5. Click **Add**.
   The notification is created and displayed on the **Notifications** page.

Copying a Notification

To copy a notification:

1. From the Service Insight navigation tree, select **Insight Central** > **Notifications**.

   The **Manage Notifications** page displays the notifications. For descriptions about the fields on this page see Table 11 on page 52.

2. Select the notification whose attributes you want to copy to create another notification.

3. Right-click your selection or use the **Actions** list and select **Copy**.

   The **Notifications** dialog box displays the attributes of the selected notification.

4. Make your modifications to the name, applied filters, and the actions. The trigger field cannot be modified. By default, the word Copy is added as a prefix to the name of the notification.

5. Click **Copy**.
   The notification is created and listed in the Notifications page.

Table 11: Manage Notifications Page Field Description

Field	Description	Range/Length
Name	Enter the name of the notification.	64 characters
Trigger Type	Select the type of trigger required to activate the notification. The fields in the Apply Filter section change dynamically according to the trigger type that you select.	• New EOL Match • New PBN Arrival • New PBN Match
Apply Filters		
Includes Tag	Select a value from the list that displays the tags that you can specify. Service Insight sends a notification when the specified trigger type contains this tag. When a public tag that is set as a filter level for a notification is deleted, the notification continues to be displayed on the Manage Notifications page with its status changed to Disabled. You are notified of this change when the notification is triggered.	255 characters
Device Name	Enter a value in the Device Name field. Service Insight sends a notification if the name of the device associated with the EOL or PBN that triggered the notification matches the entered value.	255 characters
Serial Number	Enter a value in the Serial Number field. Service Insight sends a notification if the serial number of the device associated with the EOL or PBN that triggered the notification matches the entered value.	255 characters
Has the words	Enter a value in the **Has the words** field. Service Insight sends a notification if the specified words match the words in the title of the PBN that triggered the notification. This field appears only when you select the **New PBN Arrival** trigger type.	255 characters
Does not have	Enter a value in the **Doesn't have** field. Service Insight sends a notification if the specified words do not match any of the words in the title of the PBN that triggered the notification. This field appears only when you select the **New PBN Arrival** trigger type.	255 characters
Actions		
Send Email to	Specify the e-mail addresses of users who must receive an alert when the notification is triggered and matches the specified filters. To add a new e-mail address to the list, click **Add Email**. Click the **Enter Email Id** field to enter the e-mail address. The e-mail address should be in the format user@example.com. To delete an e-mail address from the list, select the e-mail address and click **Delete**.	65535 characters
Send SNMP Traps to	Specify the destinations where SNMP traps can be sent when the notification is triggered and matches the specified filters. See Adding an SNMP Server.	Not applicable.

Related Documentation

- Targeted PBNs Overview on page 23
- Enabling and Disabling Notifications on page 53

Editing the Filters and Actions of a Notification

You can edit notification parameters, such as the applied filters, and the actions that a notification takes.

To edit a notification:

1. From the Service Insight navigation tree, select **Insight Central** > **Notifications**.

   The **Manage Notifications** page displays the notifications.

2. Select the notification whose filters and actions you want to edit.

3. Right-click your selection or use the **Actions** list and select **Edit Filters and Actions**.

   The **Notifications** dialog box displays the parameters specified for the notification.

4. Make your modifications and click **Save** to save your changes.

   To verify that your changes are saved, view the details of the notification on the Notifications page.

Related Documentation

- Targeted PBNs Overview on page 23
- Creating and Copying a Notification on page 50
- Enabling and Disabling Notifications on page 53

Enabling and Disabling Notifications

You can change the functional status of a notification from enabled to disabled, and vice versa. When you create a notification, by default, the notification is in the enabled status where it performs its functions normally. Although the notifications that you disable are inactive and do not perform the specified actions, they are listed on the Manage Notifications page and can be enabled whenever required.

When a public tag that is set as a filter level for a notification is deleted, the notification continues to be displayed on the Manage Notifications page with its status changed to Disabled. You are notified of this change when the notification is triggered.

To enable or disable a notification:

1. From the Service Insight navigation tree, select **Insight Central** > **Notifications**.
   The **Manage Notifications** page displays the notifications.

2. Select the notifications whose status you want to modify.

3. Right-click your selection or use the **Actions** list and select **Enable/Disable**.

The Change Notification Status dialog box displays the list of notifications and the changed functional status.

4. Click **Change Status** to confirm.
   The status of the selected notifications is modified.

Related Documentation

- Targeted PBNs Overview on page 23
- Creating and Copying a Notification on page 50

Deleting Notifications

You can delete multiple notifications from the Manage Notifications page.

To delete notifications:

1. From the Service Insight navigation tree, select **Insight Central** > **Notifications**.
   The **Manage Notifications** page displays the notifications.
2. Select the notifications that you want to delete.
3. Right-click your selection or use the **Actions** list and select **Delete**.
   The **Delete Notification** dialog box displays the list of selected notifications.
4. Click **Delete** to confirm.
   The selected notifications are deleted from the Service Insight database. To verify that the selected notifications are deleted, view the notifications displayed on the **Manage Notifications** page.

Related Documentation

- Targeted PBNs Overview on page 23
- Creating and Copying a Notification on page 50
- Enabling and Disabling Notifications on page 53