



Junos Space

Service Now — Service Central

Release 1.1

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Published: 2010-11-08

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos Space Service Now User Guide

Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History

December 2009—Revision 1, Junos Space Release 1.1

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE, EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

Chapter 1	Service Central Overview	1
	Service Central Overview	1
Chapter 2	Incidents	3
	Incidents Overview	3
	Assigning an Incident Owner	4
	Flagging an Incident to a User	5
	Checking Incident Status Updates	5
	Exporting Incident Data	6
	Deleting an Incident	7
	Submitting an Incident to Juniper Support Systems	7
	Viewing Incident Details	8
	Viewing a Case in the Case Manager	8
	Modifying Submit Case Options	9
Chapter 3	Information	11
	Device Snapshot Overview	11
	Exporting Device Data into HTML	12
	Deleting an iJMB	12
	Viewing iJMB Details	13
	Messages Overview	13
	Assigning an Information Message Owner	14
	Deleting Information Messages	14
	Flagging an Information Message to Users	15
	Scanning iJMBs for Impact	15
Chapter 4	Notifications	17
	Notification Policies Overview	17
	Creating and Editing a Notification Policy	18
	Enabling or Disabling a Notification Policy	22
	Deleting a Notification Policy	22

Chapter 1

Service Central Overview

- Service Central Overview on page 1

Service Central Overview

In Service Now, incidents are problem events that are detected in a device and deposited into an archive location on the Junos Space platform. When an event occurs on a device, AI-Scripts installed on that device create files called Juniper Message Bundles (JMBs) that contain comprehensive information about the device identity, the problem event, and diagnostics. The JMB file is then transferred securely from the device to the archive location. Service Now routinely polls these archive locations for new incidents and displays the incidents on the Incidents page.

After reviewing an incident, you can use the Incidents task to submit an incident case to the Juniper Support Systems (JSS) to create a Juniper Technical Assistance Center (JTAC) case. You can also notify users of the incident, assign a user as an owner of the incident, and delete the incident from the platform.

In addition to reporting incidents, AI-Scripts also send device information regularly to the archive location in the form of Information Juniper Message Bundles (iJMBs). The iJMBs are then processed and displayed on the Device Snapshot page. You can upload these iJMBs to JSS, where they are processed and analyzed to provide preventive analysis and alerts. Using Service Now, the content of these iJMBs can be viewed and can be exported in HTML format.

You can use a notification policy to specify the events for which you want to receive a notification. The options are New Incident Detected, Case Submitted, Case Status Updated, and Intelligence Update Received. Notification policies also define other characteristics (filters) that allow you to fine tune the conditions under which you receive a notification. You can even define the events that trigger the notification, the filters that further specify the trigger events, and the actions that Service Now must take after the event is triggered.

The Service Central page graphically displays information about the severities and priorities of incidents and the incidents created by you. Using Service Central you can perform the following tasks:

- Assign an owner, flag to users, update status of, and delete incidents.
- View and delete iJMBs, and export device data into HTML format.

- Assign an owner, flag to users, and delete an information message.
- Create, edit, and delete a notification policy.

Related Topics

- Incidents Overview on page 3
- Device Snapshots Overview on page 11
- Messages Overview on page 13
- Notification Policies Overview on page 17

Chapter 2

Incidents

- Incidents Overview on page 3
- Assigning an Incident Owner on page 4
- Flagging an Incident to a User on page 5
- Checking Incident Status Updates on page 5
- Exporting Incident Data on page 6
- Deleting an Incident on page 7
- Submitting an Incident to Juniper Support Systems on page 7
- Viewing Incident Details on page 8
- Viewing a Case in the Case Manager on page 8
- Modifying Submit Case Options on page 9

Incidents Overview

The Incidents page displays the incidents that were received by Service Now from devices that have AI-Scripts installed. Incidents are problem events that are detected in a device and deposited into an archive location on the Junos Space platform. These archive locations are directories on the local file system. The AI-Scripts installed on the device create files called Juniper Message Bundles (JMBs) that contain comprehensive information about the device identity, the problem event, and diagnostics. The JMB file is securely transferred from the device to the archive location. Service Now routinely polls these archive locations for new incidents. The Service Now Incidents page provides a user interface to view incidents chronologically, by organization name, and by device group.

The Incidents page also displays the JSS Technical Support cases for all Site IDs. Site IDs denote the customer identity used in the JTAC Clarify trouble ticketing system. The Technical Support user interface is available in standard controller modes. In order to receive notifications from Service Now, you must have a user account in Service Now and set up a notification policy.

When an incident, such as a process crash, an ASIC error, or a fan failure, occurs on a device that has AI-Scripts enabled, an AI-Script is executed. The AI-Script builds a JMB file with the incident data and forwards it to the Junos Space server. The JMB file is an XML file that contains diagnostic information about the device and other information specific to the condition that triggered the event message. Service Now regularly monitors the archive locations for new JMBs. If it detects a new JMB, Service

Now processes the incident and makes it available in the Service Now application. Service Now then notifies the users of the new incident. The incident contains information such as hostname, time stamp of the incident, synopsis, description, chassis serial number of the device, and the severity and priority of the incident.

You can display incidents either as thumbnails or arranged in a table. If you choose to display incidents in a table, the Service Now Incidents page lists them by incident ID, organization, device group, defect type, platform type, time of occurrence, owner, submission status, and incidents that are flagged to you. You can select which parameters to display and sort them in ascending or descending order.

You can perform the following tasks from the Incidents page:

- Submit a case so that a JTAC case is created
- Flag the incident to another user
- Assign the incident to another user
- Delete an incident
- View the details of a Juniper Message Bundle (JMB)
- View a case in the Juniper Case Manager
- Remove a flag from the incident
- Add an e-mail address to the mailing list of an incident
- View tech support cases

Related Topics

- Assigning an Incident Owner on page 4
- Flagging an Incident to a User on page 5
- Checking Incident Status Updates on page 5
- Deleting an Incident on page 7

Assigning an Incident Owner

You can assign an incident to a Junos Space user. The user to whom the incident is assigned will now own the incident. The owner is responsible for keeping track of the progress of a case or updates from JSS.

To assign an incident to a Service Now user:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents page is displayed.
2. Select the incident for which you want to assign an owner.
3. Click **Assign Ownership** from the Actions panel. The Assign Ownership dialog box is displayed.
4. Enter the login ID of the user to whom you want to assign the incident.
5. Click **Submit**. The incident is assigned to the specified user.

- Related Topics**
- Incidents Overview on page 3
 - Flagging an Incident to a User on page 5

Flagging an Incident to a User

You can flag an incident to a user who might be affected by the incident or needs to be aware of updates to it. When changes are made to this incident, the user receives an e-mail. If an incident is flagged to you, the Flag column of that incident in the Incidents table displays **Yes**. If not, it displays **No**.

To flag an incident to a user:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents table is displayed.
2. Select the incident that you want to flag to a user.
3. Click **Flag to Users** from the Actions panel. The Flag to Users dialog box displays the names of Service Now users.
4. Select the user or users to whom you want to flag the incident.
5. Click **Submit**. The incident is flagged to the selected users.

To clear a flag, uncheck the user from the **Flag to Users** dialog box.

- Related Topics**
- Incidents Overview on page 3
 - Assigning an Incident Owner on page 4

Checking Incident Status Updates

In Service Now, incidents are problem events that are detected in a device. Information about these incidents is sent to the device archive locations. These archive locations are directories on the local file system. Service Now routinely polls these archive locations for new incidents. The Service Now Incidents page provides a user interface to view incidents chronologically by organization name and device group.

You can use the Incidents page to submit an incident so that a Juniper Technical Assistance Center (JTAC) case is created. The submission status of the incident is displayed in the Status column in the Incidents page. After you submit the incidents, the status is **Submitted**. When the case is created by JSS, the status changes to **Created** and the Case ID appears. Further updates to the incident will change the incident status to **Updated**.

Service Now provides three ways to check incident status.

- Using Junos Space logs. The Junos Space log of an incident displays a list of the status changes.

- Using notification policies. You can create a notification policy to notify users whenever the status of an incident is updated. For more information about creating notification policies, see “Creating and Editing a Notification Policy” on page 18.
- Using the landing page of Service Central. The My Incidents box, on the landing page of Service Central displays the number of incidents whose status has changed since you last logged in. It also displays other information such as the number of incidents that were flagged to you, the number of incidents that you own, and the number of new incidents that were added since your last log in. To view the landing page of the Service Central, select **Service Central** from the Service Now task ribbon.

- Related Topics**
- Incidents Overview on page 3
 - Assigning an Incident Owner on page 4

Exporting Incident Data

You can export incident data into HTML and Excel file formats and share it on your local file system.

To export incident data into HTML format:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents page is displayed.
2. Select the device whose incident details you want to export.
3. Click **Export JMB to HTML** from the Actions panel. The Export JMB to HTML dialog box displays links to the original and filtered JMBs.
4. Click a link to save the JMB file as HTML.

To export JMB data into Excel file format:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents page is displayed.
2. Select the incident whose details you want to export. To select more than one incident, use the **Multiple** tab.
3. Click **Export Incident Summary to Excel** from the Actions panel. The Export Incident Summary to Excel dialog box displays a link to the Excel file.
4. Click the link to save the incidents in Excel format

- Related Topics**
- Incidents Overview on page 3
 - Assigning an Incident Owner on page 4
 - Flagging an Incident to a User on page 5

Deleting an Incident

After reviewing the incident information, you can use the Incidents page to delete incidents from Service Now. This action deletes the incident both from the Service Now database and from the Incidents table.

To delete an incident:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents table is displayed.
2. Select the incident that you want to delete.
To select more than one incident, use the **Multiple** tab.
3. Click **Delete**. The selected incidents are removed from the Incidents table and the Service Now database.

- Related Topics**
- Incidents Overview on page 3
 - Flagging an Incident to a User on page 5

Submitting an Incident to Juniper Support Systems

After reviewing the incident information, you can use the Incidents page to submit an incident to create a Juniper Technical Assistance Center (JTAC) case. You can submit multiple cases to JSS simultaneously. The submission status of the incident is displayed in the Status column in the Incidents page. After you submit the incident, the status is **Submitted**. When the case is created by JSS, the status changes to **Created** and the Case ID appears.

To submit a case:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents page is displayed.
2. Select the incident for that you want to submit a case. To select multiple incidents, use the **Multiple** tab
3. Click **Submit Case** from the Actions panel. The Submit Case dialog box displays the device name, and incident synopsis. The Submit Case action will be disabled when you select an incident that is already submitted.

Device	Synopsis
Test	ACCT_MALLOC_FAILURE

4. Click **Submit** to submit the case to create a JTAC.

The Incidents page displays the submission status in the Status column. Thereafter, the status is **Submitted**. When the case is created by JSS, the status changes to **Created** and the Case ID appears.

- Related Topics**
- Incidents Overview on page 3
 - Flagging an Incident to a User on page 5

Viewing Incident Details

When incidents are received, only selected information is displayed on the Incidents page. Service Now allows you to view the entire content of the incident.

To view incident details:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents page is displayed.
2. Select the incident whose details you want to view.
3. Click **View JMB** from the Actions panel. A View JMB dialog box displays links to the original and filtered JMB details.
4. Click a link. This new window displays the details of the selected incident.

- Related Topics**
- Incidents Overview on page 3
 - Flagging an Incident to a User on page 5

Viewing a Case in the Case Manager

You can view the details of a submitted case in the Juniper Networks Case Manager. To view case details in the Case Manager, you must first have a user Id and password for the Juniper Networks Customer Support Center (CSC). You can request the user Id and password at <http://www.juniper.net/customers/support/> or by contacting Juniper Customer Care.

To view a case in the Case Manager:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents page is displayed.
2. Select the incident whose details you want to view in the Case Manager.
3. Click **View Case in Case Manager** from the **Actions** panel. If the **View Case in Case Manager** link is not enabled, ensure that the case has been created. The Juniper Networks Login page is displayed.
4. Enter your user name and password and click **Login**. The JSS Case Manager displays the case details.



NOTE: You can also view the details of the submitted cases in the Case Manager from the View Tech Support Cases page. To view case details, go to **Service Central > Incidents > View Tech Support Cases** and follow steps 2 to 4 from the above procedure.

- Related Topics**
- Incidents Overview on page 3
 - Flagging an Incident to a User on page 5

Modifying Submit Case Options

For any incident in Service Now, you can modify submit case settings such as the case priority and the e-mail list associated with a case.

To modify submit case options:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The Incidents table is displayed.
2. Select the incident whose submit case options you want to modify.
3. Click **Modify Submit Case Options** from the Actions panel. The Modify Submit Case Options dialog box is displayed.
4. Make your changes and click **Submit**. The settings are saved in the Service Now database.

- Related Topics**
- Incidents Overview on page 3
 - Submitting an Incident to Juniper Support Systems on page 7

Chapter 3

Information

- Device Snapshot Overview on page 11
- Exporting Device Data into HTML on page 12
- Deleting an iJMB on page 12
- Viewing iJMB Details on page 13
- Messages Overview on page 13
- Assigning an Information Message Owner on page 14
- Deleting Information Messages on page 14
- Flagging an Information Message to Users on page 15
- Scanning iJMBs for Impact on page 15

Device Snapshot Overview

Service Now polls device archive locations regularly to receive Information Juniper Message Bundles (iJMBs) that contain information about devices. These iJMBs are then processed and displayed on the Device Snapshot page in the Service Now application. You can upload these iJMBs to JSS, where they will be added to the Customer Intelligence Database (CIDB) database, and will be processed and analyzed to provide preventive measures.

You can also filter the configuration content from an iJMB before sending it to JSS, with the help of Service Now global settings, and then track the status of the iJMB submission to JSS.



NOTE: When you upgrade from Junos Space 1.1, the destination URL configured on devices is invalid and JMBs are not sent to Service Now. To be able to receive JMBs, AI-Scripts must be reinstalled on all devices. See [Installing AI-Scripts on Devices Using Service Now](#).

You perform the following tasks using the Information Device Snapshot tab:

- Exporting Device Data into HTML
- Deleting an iJMB
- Viewing iJMB Details

- Related Topics**
- Exporting Device Data into HTML on page 12
 - Viewing Device Snapshot Details on page 13
 - Messages Overview on page 13

Exporting Device Data into HTML

Device data collected by Service Now and displayed on the Device Snapshot page can be exported in HTML format.

To export device data in HTML format:

1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshot**. The Device Snapshot page is displayed.
2. Select the organization whose data you want to export.
3. Click **Export to HTML** from the **Actions** panel. The Export JMB to HTML dialog box displays links to the original and filtered versions of the JMB.
4. Click a link to save the iJMB as HTML.

- Related Topics**
- Messages Overview on page 13
 - Viewing Device Snapshot Details on page 13

Deleting an iJMB

Device data that is collected by Service Now and displayed on the Device Snapshot page can be deleted from the Service Now database.

To delete an iJMB:

1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshot**. The Device Snapshot page is displayed.
2. Select the organization whose device information you want to delete. If you want to delete data from more than one organization, use the **Multiple** tab.
3. Click **Delete** from the Actions panel. Click **Delete** again to confirm deletion. The iJMBs from the selected organizations will be deleted from the Service Now database and they will no longer appear on the Device Snapshot page.

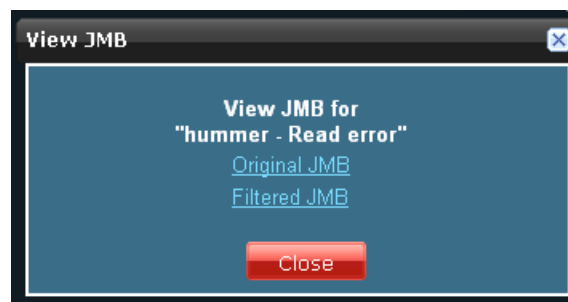
- Related Topics**
- Messages Overview on page 13
 - Viewing Device Snapshot Details on page 13

Viewing iJMB Details

When iJMBs are received by Service Now, only selected information is displayed on the Device Snapshot page. The entire content of an iJMB can be viewed using Service Now.

To view the details of an iJMB:

1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshot**. The Device Snapshot page is displayed.
2. Select the organization whose iJMB contents you want to view.
3. Click **View JMB** from the **Actions** panel. The View JMB dialog box shows links to the original and the filtered iJMB details page. The information in the filtered JMB is classified by the settings on your Global Settings page.



4. Click a link. A new window displays the iJMB details.

Related Topics ■ Messages Overview on page 13

Messages Overview

Service Now polls JSS regularly to receive information messages for every configured organization. These information messages are displayed on the Service Now Messages page. Using Service Now, every information message can be assigned an owner and flagged to users. This ensures that users are kept informed of changes made to information messages.

You perform the following tasks using the Information Messages tab:

- Assigning an information message owner
- Flagging an information message to users
- Deleting information messages
- Scanning for affected devices

- Related Topics**
- Device Snapshots Overview on page 11
 - Assigning Ownership on page 14
 - Flagging a Message to Users on page 15
 - Deleting a Message on page 14

Assigning an Information Message Owner

You can assign every information message to a Junos Space user who needs to be notified.

To assign an owner (Junos Space user) to an information message:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**. The Messages page is displayed.
2. Select the information message to which you want to assign an owner.
3. Click **Assign Ownership** from the Actions panel. The Assign Ownership dialog box is displayed.
4. Enter the Login ID of the Junos Space user.
5. Click **Submit**. The specified user will be assigned ownership of the selected information message.

- Related Topics**
- Device Snapshots Overview on page 11
 - Flagging a Message to Users on page 15

Deleting Information Messages

Information messages that are collected by Service Now and displayed on the Messages page can be deleted from the Service Now database.

To delete an information message:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**. The Messages page is displayed.
2. Select the information message that you want to delete. To delete more than one information message, use the **Multiple** tab.
3. Click **Delete** from the Actions panel. Click **Delete** again to confirm deletion. The selected information messages will be deleted from the Service Now database and they will no longer appear on the Messages page.

- Related Topics**
- Device Snapshots Overview on page 11
 - Messages Overview on page 13

Flagging an Information Message to Users

You can flag an information message to a Junos Space user who you think needs to keep track of the information message or who needs to be notified when it is changed.

To flag an information message to a user:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**. The Messages page is displayed.
2. Select the information message that you want to flag to a user.
3. Click **Flag to Users** from the Actions panel. The Flag to Users dialogues box lists the available users.
4. Select one or more users who must be notified of the selected information message.
5. Click **Submit**. The specified users will be notified of the selected information message. The selected information message will be flagged to them, and the **Flag** column of that information message displays **Yes**.

- Related Topics**
- Device Snapshots Overview on page 11
 - Messages Overview on page 13

Scanning iJMBs for Impact

Service Now allows you to view the devices impacted by the vulnerabilities described in the inform message.

To scan iJMBs and view the impacted devices:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**. The Messages page is displayed.
2. Select the message that you want to scan for impact.
3. Click **Scan for Impact** from the Actions panel. The Scan for Impact Results page displays the list of devices that are impacted by the selected message. If no devices are impacted by the selected message, the following message is displayed: **No impacted devices found**.

- Related Topics**
- Messages Overview on page 13
 - Viewing Device Snapshot Details on page 13

Chapter 4

Notifications

- Notification Policies Overview on page 17
- Creating and Editing a Notification Policy on page 18
- Enabling or Disabling a Notification Policy on page 22
- Deleting a Notification Policy on page 22

Notification Policies Overview

In Service Now, a notification policy specifies the events that you want Service Now to send a notification and also the actions you want taken. Service Now sends you a notification when a specific event occurs. Notification policies define the parameters for these notifications.

You can specify the following parameters when you create a notification policy

- Trigger—Specify the event that causes Service Now to send the notification.
- Filters—Further specify the events that cause Service Now to send a notification.
- Actions—Specify the action (or actions) that must be taken after the specified event is triggered. These events can be filtered by priority, device name, serial number, and so on. Different filters are supported for incident and information trigger types.

Service Now provides an interface where you can manage these notification policies. The Notifications page displays the notification policies chronologically by name, owner, status, and trigger. For more information about the Notifications table columns, see Table 1 on page 17.

Table 1: Notification Policies Table Column Descriptions

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Name	Name of the policy, which must be unique among all policies owned by the same user.	Hyperlink requires Notification Policy privilege	64 characters	N/A
Owner	Name of the user who owns the notification policy.	N/A	N/A	N/A
Status	Whether the notification policy is running.	N/A	Enabled or Disabled	N/A

Table 1: Notification Policies Table Column Descriptions *(continued)*

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Trigger Type	Type of trigger that should occur in order for the notification policy to be applied.	N/A	<ul style="list-style-type: none"> ■ New Incident Detected ■ Incident Submitted ■ Case ID Assigned ■ Case Status Updated ■ New Information Update 	N/A

- Related Topics**
- Creating and Editing a Notification Policy on page 18
 - Enabling or Disabling a Notification Policy on page 22
 - Deleting a Notification Policy on page 22

Creating and Editing a Notification Policy

You can create a notification policy that specifies the circumstances on which you want Service Now to send notifications, and who notifications should be sent to. You can define the events that trigger the notification, the filters that further specify the trigger events, and the actions that Service Now must take after the event is triggered.

To create a notification policy:

1. From the Service Now task ribbon, select **Service Central** > **Notifications** > **Create Notifications**. The Create Notifications page is displayed.

2. Enter a notification policy name and select a trigger.
3. Enter filter parameters. Different filters are supported for incident and information trigger types.
4. Enter the information for the users who should receive notifications.

For more information about the fields in the Create Notification Policy dialog box, see Table 2 on page 20.

You can also edit the trigger events, filters, and actions of an existing notification policy.

To modify a notification policy:

1. From the Service Now task ribbon, select **Service Central** > **Notifications** > **Create Notifications**. The Create Notifications page is displayed.
2. From the Notifications table, select the notification policy that you want to edit and click **Edit filters and Actions**. The Create Notifications page is displayed.
3. Edit the desired fields. See Table 2 on page 20, and for more information see Table 3 on page 21.

Table 2: Create Notification Policy Page Field Descriptions

Field	Description	Range/Length	Default
Name	Name of the policy, which must be unique among the policies owned by the same user.	64 characters	N/A
Trigger Type	Type of trigger required to activate this policy. The fields in the filter table dynamically change according to the selected trigger type.	<ul style="list-style-type: none"> ■ New Incident Detected ■ Incident Submitted ■ Case ID Assigned ■ Case Status Updated ■ New Information Update 	N/A
Apply Filters:			
Common Filter Parameters:			
Priority	Select a value in the Priority field. Service Now will send a notification if the priority of the incident matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Device Name	Enter a value in the Device Name field. Service Now will send a notification if the name of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Serial Number	Enter a value in the Serial Number field. Service Now will send a notification if the serial number of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Has the words	Enter a value in the Has the words field. Service Now will send a notification if the specified words match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Doesn't have	Enter a value in the Doesn't have field. Service Now will send a notification if the specified words do not match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Information Trigger Type Notification Policy Filter Parameters:			
Information Update Type	Enter a value in the Information Update Type field. Service Now will send a notification if the type of information message update matches the entered value.	255 characters	Blank
Products Affected	Enter a value in the Products Affected field. Service Now will send a notification if the Products Affected field value in alert information messages matches the entered value	255 characters	Blank

Table 2: Create Notification Policy Page Field Descriptions *(continued)*

Field	Description	Range/Length	Default
Platform Type	Enter a value in the Platform Type field. Service Now will send a notification if the Platforms Affected field in alert information messages or the platform type field in information messages match the entered value	255 characters	Blank
Keywords	Enter a value in the Keywords field. Service Now will send a notification if the Keyword in information messages matches the entered value	255 characters	Blank
Software Version	Enter a value in the Software Version field. Service Now will send a notification if the software version in the information messages matches the entered value	255 characters	Blank
Hardware Version	Enter a value in the Hardware Version field. Service Now will send a notification if the hardware version in the information messages matches the entered value	255 characters	Blank
Devices Impacted	Enter a value in the Devices Impacted field. Service Now will send a notification if the devices impacted in the information messages matches the entered value	255 characters	Blank
Actions:			
Send Email to	<p>Displays the list of e-mail addresses that receive a message if the policy is triggered and passes the specified filter.</p> <p>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.</p> <p>To delete an e-mail address from the list, select the e-mail address and click Delete</p>	65535 characters	Blank
Send Traps to	An SNMP trap is sent to the destinations that are selected if an event occurs and passes the specified filter. See Adding an SNMP Server	N/A	N/A

Table 3: Notification Policy Table Command Button Descriptions

Element Name	Description	Privilege Required	Results
Edit filters and actions	Opens the Create Notification page, where you can edit the filters and actions of the selected notification policy.	Notifications	Opens the Create Notification page
Copy	Opens the Create Notification page, where you can create a copy of the selected notification policy.	Notifications	Opens the Create Notification page
Delete	Deletes the selected notification policy	Notifications	Removes the selected policies from the table
Change Status	Opens the Change Notification Policy Status dialog box, where you can change the status of a notification policy from Enabled to Disabled or vice versa.	Notifications	Status of selected policies is changed from Enabled to Disabled or vice versa

- Related Topics**
- Notification Policies Overview on page 17
 - Enabling or Disabling a Notification Policy on page 22

Enabling or Disabling a Notification Policy

You can enable a notification policy that specifies the events for which Service Now sends a notification, and the actions that Service Now should take in response to these events. The notification policy defines the events that trigger the notification, the filters that further specify the trigger events, and the actions that Service Now must take after the event is triggered.

To enable a notification policy:

1. From the Service Now task ribbon, select **Service Central** > **Notifications**. The Notifications page is displayed.
2. Select the notification policies whose status you wish to change. To select more than one notification policy, use the **Multiple** tab.
3. Click **Change Status** from the Actions panel. Click **Change Status** again to confirm your action. The status of the notification policy changes from **Enabled** to **Disabled** or vice versa.

- Related Topics**
- Notification Policies Overview on page 17
 - Creating and Editing a Notification Policy on page 18

Deleting a Notification Policy

You can delete an existing notification policy that specifies the events for which Service Now sends a notification, and the actions that Service Now should take in response to these events. The notification policy defined the events that trigger the notification, the filters that further specified the trigger events, and the actions that Service Now took after the event was triggered.

To delete a notification policy:

1. From the Service Now task ribbon, select **Service Central** > **Notifications**. The Notifications page is displayed.
2. From the Notifications table, select the notification policy (or policies) that you wish to delete. To delete more than one notification policy, use the **Multiple** tab.
3. Click **Delete**. The **Confirm Deletion of Notification Policies** dialog box displays the name of the notification policy and its owner.
4. Click **Delete**. This action deletes the selected notification policies from the Service Now database and from the Notifications table.

- Related Topics**
- Notification Policies Overview on page 17
 - Enabling or Disabling a Notification Policy on page 22

