



Junos Space

Service Now — Service Central

Release

1.4



Published: 2010-08-20

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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
August 2010—Junos Space Release 1.4, Revision 1

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

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The 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

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	6
	Exporting Incident Data	6
	Deleting an Incident	7
	Submitting an Incident to Juniper Support Systems	8
	Viewing Incident Details	8
	Viewing a Case in the Case Manager	9
	Modifying Submit Case Options	10
	Updating an End Customer Case	11
Chapter 3	Information	13
	Messages Overview	13
	Assigning Ownership	14
	Flagging a Message to Users	14
	Deleting a Message	15
	Scanning a Message for Impact	15
	Assigning a Message to a Connected Member	15
	Device Snapshots Overview	17
	Exporting Device Data into HTML	17
	Deleting Device Snapshots	18
	Viewing Device Snapshot Details	18
Chapter 4	JMB Errors	21
	JMB Errors	21
	Downloading JMB Errors	21
	Deleting JMB Errors	22
Chapter 5	Notifications	23
	Notification Policies Overview	23
	Creating and Editing a Notification Policy	24
	Enabling or Disabling a Notification Policy	28
	Deleting a Notification Policy	29
Chapter 6	Index	31
	Index	33

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 sent to the Service Now application. When an event occurs on a device, 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 then transferred securely from the device to Service Now. Service Now searches for new incidents and displays the incidents on the **Manage 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 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 Service Now in the form of Information Juniper Message Bundles (iJMBs). The iJMBs are then processed and displayed on the **Manage Device Snapshots** page. You can upload these iJMBs to JSS, where they are processed and analyzed to provide preventive analysis and alerts. Using Service Now, you can view the content of these iJMBs and export them in HTML format.

In Service Now, JMB errors are JMBs that do not comply with the standard data structure that Service Now requires or that contain data elements that Service Now does not accept. Service Now identifies these JMBs and displays them on the **Manage JMB Errors** page where you can view and download them.

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 define other characteristics (filters) that you can use 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 you want Service Now to take after the event is triggered.

Some tasks under the Service Central workspace, such as assigning messages to a connected member and updating an end customer case, are enabled only when the

Service Now end customer mode is activated. For more information on the Service Now modes, see [Service Now Modes](#).

The **Service Central** page graphically displays information about the severity and priority of incidents and the incidents you created.

Using Service Central you can perform the following tasks:

- Assign an incident owner, flag incident to users, update status of, and delete incidents.
- View and delete iJMBs, and export device data into HTML format.
- Assign messages to end customers (enabled if you are a Service Now partner).
- Update end customer cases (enabled if you are a Service Now partner).
- View, download, and delete JMBs with errors.
- Assign an owner, flag to users, and delete an information message.
- Create, edit, and delete a notification policy.

Related Topics

- [Service Now Modes](#)
- [Incidents Overview on page 3](#)
- [Device Snapshots Overview on page 17](#)
- [Messages Overview on page 13](#)
- [JMB Errors on page 21](#)
- [Notification Policies Overview on page 23](#)

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 6
- Exporting Incident Data on page 6
- Deleting an Incident on page 7
- Submitting an Incident to Juniper Support Systems on page 8
- Viewing Incident Details on page 8
- Viewing a Case in the Case Manager on page 9
- Modifying Submit Case Options on page 10
- Updating an End Customer Case on page 11

Incidents Overview

In Service Now, Incidents are problem events that are detected on a device. When an incident, such as a process crash, an ASIC error, or a fan failure, occurs on an AI-Scripts-enabled device, the AI-Script builds a JMB file with the incident data and forwards it to the Junos Space server. AI-Scripts create files called Juniper Message Bundles (JMBs).

A 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. 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.

These JMB files are securely transferred from the device to the Service Now application. After a JMB is generated, the device automatically initiates a file transfer to Service Now and the incident is displayed on the **Manage Incidents** page.

Service Now uses Device Management Interface (DMI), which is an extension to the NETCONF network management protocol, to receive JMBs from devices. The **Manage Incidents** page provides a user interface to view incidents chronologically, by organization name, and by device group. The thumbnail view of this page helps you differentiate

incidents with various icons. These icons indicate incident priority levels and also whether the incidents are submitted to JSS. See [Service Now Icons](#).

From the Incidents workspace you can navigate to the **View Tech Support Cases** and **View End Customer Cases** pages. The **View Tech Support Cases** page displays the technical support cases that you open with JSS. You can open these cases only after you create an organization and the organization's site ID is validated. Site IDs denote the customer identity used in the Juniper Technical Assistance Center (JTAC) Clarify trouble ticketing system.

To stay updated of the events that occur in Service Now, you can create notification policies that instantly notify you of an event in the form of e-mails or snmp traps.

You can display incidents either as thumbnails or arranged in a table. If you choose to display incidents in a table, the **Manage 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 the ascending or descending order.

You can perform the following tasks from the **Manage Incidents** page:

- Submit an incident to create a JTAC case
- 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 Networks 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](#)
 - [Deleting an Incident on page 7](#)

Assigning an Incident Owner

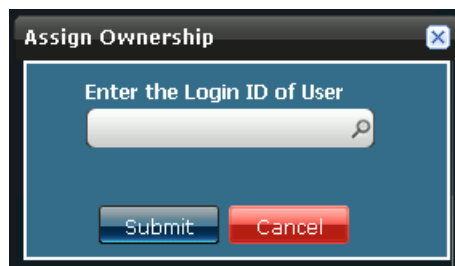
You can assign an incident to a Junos Space user, who becomes the owner of the incident. The owner is responsible for keeping track of the progress of a case or updates from JSS.

To assign an incident to a Service Now user:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage 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. Click the search icon to display the list of available users.
5. Click **Submit**.

The incident is assigned to the specified user. See “Viewing Device Snapshot Details” on page 18

- 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 Manage 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.

- 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 Service Now application. Service Now routinely checks for new incidents. The Service Now **Manage Incidents** page provides a user interface to view incidents chronologically by organization name and device group.

You can use the **Manage 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 **Manage Incidents** page. After you submit the incidents, the status is **Submitted**. When JSS creates the case, the status changes to **Created** and the Case ID appears. Further updates to the incident change the incident's 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 24.
- Using the Service Central page. The My Incidents graph on the Service Central page 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 login. To view the Service Central page, 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 save it on your local file system.

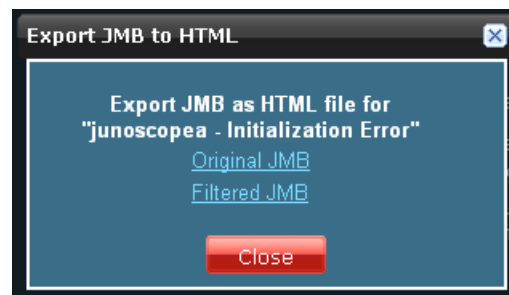
Exporting Incident Data into HTML

To export incident data into HTML format:

1. From the Service Now task ribbon, select **Service Central > Incidents**. The **Manage 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, as shown in Figure 1 on page 7.

Figure 1: Export JMB to HTML Dialog Box



4. Click a link to save the JMB file as HTML.

Exporting Incident Data into Excel

To export JMB data into Excel file format:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage Incidents** page is displayed.
2. Select the incident whose details you want to export.
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 displayed 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 **Manage 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.
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

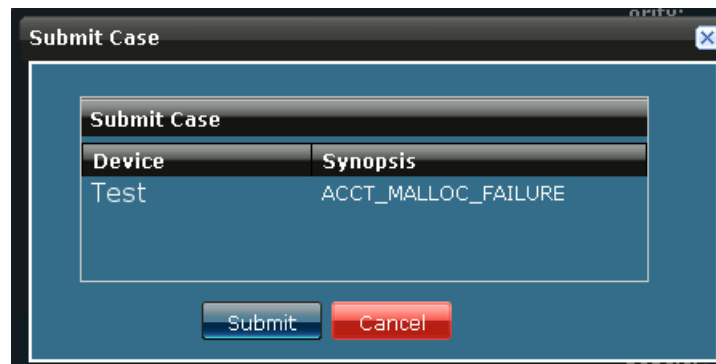
Submitting an Incident to Juniper Support Systems

After reviewing the incident information, you can use the **Manage Incidents** page to submit an incident to create a case. You can submit multiple cases to Juniper Support Systems (JSS) simultaneously. The submission status of the incident is displayed in the **Status** column in the **Manage 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 an incident:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage Incidents** page is displayed.
2. Select the incident for which you want to create a case.
3. Click **Submit Case** from the Actions panel.

The **Submit Case** dialog box displays the device name, and incident synopsis. The **Submit Case** action is disabled when you select an incident that is already submitted.



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

The **Manage 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 **Manage Incidents** page. Using Service Now, you can view the entire content of the incident.

To view incident details:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage Incidents** page is displayed.
2. Select the incident whose details you want to view.
3. Click **View JMB** from the Actions panel.
The **View JMB** dialog box displays links to the original and filtered JMB details.
4. Click the 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 Networks Customer Care.

To view a case in the Case Manager:

1. From the Service Now task ribbon, select **Service Central > Incidents**.
The **Manage 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, 3, and 4 from the preceding 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 the submit case settings, such as the case priority and the e-mail list associated with the case. You can also add your comments to the synopsis and the description of an incident before you submit it to JSS.

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.

Modify Submit Case Options

Add CC to Case:

Add Email **Delete**

Email List
Enter Email Id

Priority:

High

Synopsis:

RPD_ISIS_OVERLOAD

Add Comments to Synopsis:

Problem Description:

RPD_ISIS_OVERLOAD: No additional memory is available for storing IS-IS link-state information. Either system resources are exhausted or a software error occurred (such as a memory leak in the routing protocol process [rpd]).

Add Comments to Description:

Save **Save And Submit** **Cancel**

4. To enter an e-mail id click the **Enter Email Id** field.
Enter the e-mail ID in the format user@example.com. To add multiple e-mail IDs, and delete, use the **Add Email** and **Delete** buttons respectively.
5. To modify the priority of the case, click the **Priority** drop-down arrow and select one of the options.
The available options are Critical, High, Medium, and Low. The default priority is medium.

6. To add your comments to the problem description and synopsis of the case, enter your comments in the **Add Comments to Synopsis** and **Add Comments to Description** fields.
The maximum limit for the comments is 1,028 characters.
7. To save your settings in the Service Now database, click **Save**.
Your settings are saved and the **Manage Incidents** page is displayed.
8. To save your settings in the Service Now database and submit the selected incident to JSS, click **Save and Submit**.
The incident is submitted to JSS and your settings are saved in the Service Now database. You are taken to the **Manage Incidents** page.

- Related Topics**
- Incidents Overview on page 3
 - Submitting an Incident to Juniper Support Systems on page 8

Updating an End Customer Case

As a Service Now partner, you can create a case for the incident you receive from an end customer's device and also update the case.

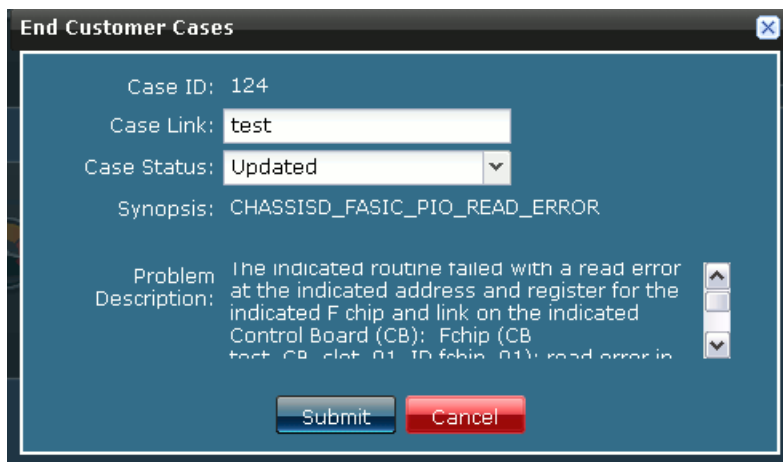


NOTE: This action is disabled when Service Now operates in end customer mode, standard mode, and demo mode. This action is also disabled when a case is closed.

To update an end customer case:

1. From the Service Now task ribbon select, **Service Central > Incidents**.
The **Manage Incidents** page displays the list of incidents.
2. Select the end customer incident for which you want to create a case.
3. Right-click your selection and select **End Customer Case**.
The **End Customer Case** dialog box is displayed as shown in Figure 2 on page 12.

Figure 2: End Customer Cases Dialog Box

A screenshot of a web-based dialog box titled "End Customer Cases". The dialog box has a blue header bar with the title and a close button. The main content area is white and contains several fields: "Case ID: 124", "Case Link: test" (with a text input field), "Case Status: Updated" (with a dropdown arrow), and "Synopsis: CHASSISD_FASIC_PIO_READ_ERROR". Below these is a "Problem Description:" section with a text area containing the text: "The indicated routine failed with a read error at the indicated address and register for the indicated F chip and link on the indicated Control Board (CB): Fchip (CB test CB slot 01 ID fchip 01): read error in". To the right of the text area are three small icons: a magnifying glass, a left arrow, and a right arrow. At the bottom of the dialog box are two buttons: "Submit" (blue) and "Cancel" (red).

You can also select **End Customer Case** from the **Actions** panel.

This **End Customer Case** action is enabled only if you select an end customer incident.

4. Modify the case details.
5. Click **Submit**.

The case is updated and sent to the Service Now end customer.

- Related Topics**
- Service Now Overview
 - Adding a Connected Member

CHAPTER 3

Information

- Messages Overview on page 13
- Assigning Ownership on page 14
- Flagging a Message to Users on page 14
- Deleting a Message on page 15
- Scanning a Message for Impact on page 15
- Assigning a Message to a Connected Member on page 15
- Device Snapshots Overview on page 17
- Exporting Device Data into HTML on page 17
- Deleting Device Snapshots on page 18
- Viewing Device Snapshot Details on page 18

Messages Overview

Service Now polls JSS regularly to receive information messages for every configured organization. These information messages are displayed on the Service Now **Manage Messages** page. Using Service Now, you can assign every information message to an owner and flag it 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 17
- Assigning Ownership on page 14
- Flagging a Message to Users on page 14
- Scanning a Message for Impact on page 15
- Deleting a Message on page 15

Assigning Ownership

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 **Manage 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 is assigned ownership of the selected information message.

- Related Topics**
- Device Snapshots Overview on page 17
 - Flagging a Message to Users on page 14

Flagging a 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** dialog 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 are notified of the selected information message. The selected information message are flagged to them, and the **Flag** column of that information message displays **Yes**.

- Related Topics**
- Device Snapshots Overview on page 17
 - Messages Overview on page 13

Deleting a Message

You can delete information messages from the Service Now database that Service Now collects and that are displayed on the **Manage Messages** page.

To delete an information message:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**.
The **Manage Messages** page is displayed.
2. Select the information message that you want to delete.
3. Click **Delete** from the Actions panel. Click **Delete** again to confirm deletion.

The selected information messages are deleted from the Service Now database and they no longer appear on the **Manage Messages** page.

- Related Topics**
- Device Snapshots Overview on page 17
 - Messages Overview on page 13

Scanning a Message for Impact

You can use Service Now 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 **Manage 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 18

Assigning a Message to a Connected Member

Service Now polls JSS regularly to receive messages for every configured organization. As a Service Now partner, you can assign multiple messages to a connected member. This action is available only when Service Now operates in partner proxy mode. For more

information about standard, partner, and end customer modes, see [Service Now Modes](#).



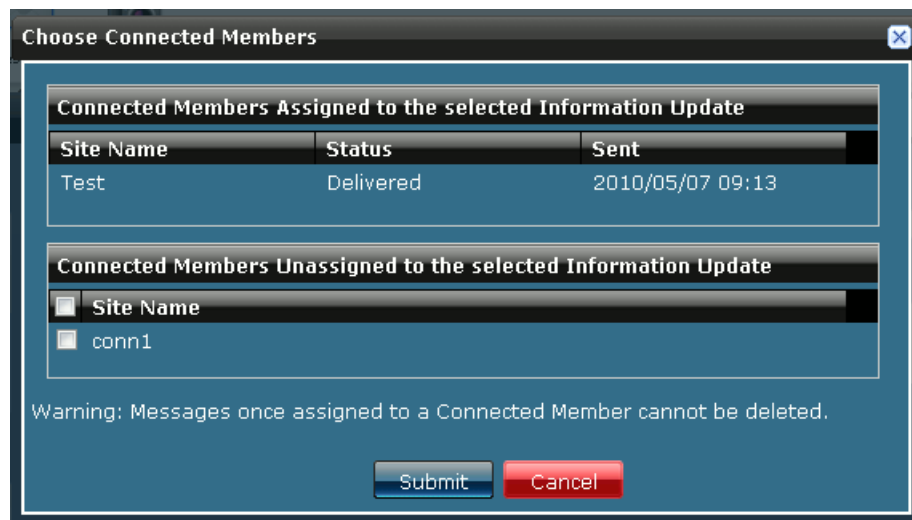
NOTE: After a message is assigned to a [Connected Member](#) it cannot be deleted.

To assign a message to a connected member:

1. From the Service Now task ribbon, select **Service Central > Information > Messages**.
The **Manage Messages** page displays the list of information messages received.
2. Select the message that you want to assign to a connected member.
3. Right-click your selection or use the **Actions** panel and select **Assign Message to End Customer**.

As shown in Figure 3 on page 16, the **Choose Connected Members** dialog box displays the list of connected members and also the connected members to whom the message is already assigned along with the status.

Figure 3: Choose Connected Members Dialog Box



4. Select the connected member to whom this message can be assigned.
5. Click **Submit**.

The selected message is assigned to the connected member. To verify this action you can navigate to the **Manage Organizations** page, and list the messages assigned to any connected member. See [Viewing Messages Assigned to a Connected Member](#).

Related Topics • [Adding a Connected Member](#)

Device Snapshots Overview

Service Now periodically collects and displays Information Juniper Message Bundles (iJMBs) that contain information about devices. These iJMBs are processed and displayed on the **Manage Device Snapshot** page in the Service Now application. You can upload these iJMBs to JSS, where they are added to the Customer Intelligence Database (CIDB) database, and then 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.

Devices that have stopped sending information (device snapshots) to Service Now for more than two weeks are also detected and graphically displayed on the Administration page. To list these devices you can click the **Devices Not Sending Snapshots** bar of the **Devices Not Sending Device Snapshots** graph. These devices are displayed on the **Service Now Devices** page where you can view their details and export them to HTML format. The thumbnail view of the **Manage Device Snapshots** page uses different icons to help you identify snapshots that have been successfully uploaded to JSS and the device snapshots whose submission to JSS failed. For a description of these icons, see Service Now Icons.

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

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

- Related Topics**
- Exporting Device Data into HTML on page 17
 - Viewing Device Snapshot Details on page 18
 - Messages Overview on page 13

Exporting Device Data into HTML

You can take device data that Service Now collects and displays on the **Manage Device Snapshots** page and export it in HTML format.

To export device data in HTML format:

1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshots**.
The **Manage Device Snapshots** page displays the device snapshots received.
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 the displayed link to save the iJMB as HTML.

- Related Topics**
- Messages Overview on page 13
 - Viewing Device Snapshot Details on page 18

Deleting Device Snapshots

You can take device data that Service Now collects and displays on the **Manage Device Snapshots** page and delete it from the Service Now database.

To delete an iJMB:

1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshots**.

The **Manage Device Snapshots** page is displayed.

2. Select the organization whose device information you want to delete.
3. Click **Delete** from the Actions panel. Click **Delete** again to confirm deletion.

The iJMBs from the selected organizations are deleted from the Service Now database and they no longer appear on the **Manage Device Snapshots** page.

- Related Topics**
- Messages Overview on page 13
 - Viewing Device Snapshot Details on page 18

Viewing Device Snapshot Details

When Service Now receives iJMBs, only selected information is displayed on the **Manage Device Snapshots** page. You can display the entire content of the iJMB using the View JMB action in Service Now.

To view the details of an iJMB:

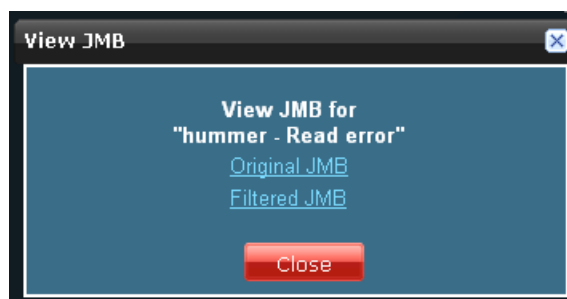
1. From the Service Now task ribbon, select **Service Central > Information > Device Snapshots**.

The **Manage Device Snapshots** 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 displays links to the original and the filtered iJMBs as shown in Figure 4 on page 19. The information in the filtered JMB is classified by the settings on your **Global Settings** page.

Figure 4: View JMB Dialog Box



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

Related Topics • Messages Overview on page 13

CHAPTER 4

JMB Errors

- JMB Errors on page 21

JMB Errors

Service Now identifies the JMBs with errors and displays them on the **Manage JMB Errors** page for monitoring purposes. You can download up to five JMB files at a time and also delete them from the Service Now database. JMBs with errors are JMBs that do not comply with the standard data structure or other data elements that Service Now accepts. We recommend that you open a case with JSS for unique error JMBs.

- Downloading JMB Errors on page 21
- Deleting JMB Errors on page 22

Downloading JMB Errors

To download the JMB errors in a zipped file:

1. From the Service Now task ribbon, select **Service Central > Incidents > JMB Errors**.

The **Manage JMB Errors** page is displayed.



2. Select the JMB whose details you want to download. You can download up to five JMB files at a time.
3. Click **Download JMB Errors** from the Actions panel.

The **Download JMB Errors** dialog box is displayed.

4. Click the **Click here to download JMB Error files** link to save the selected JMB in a zipped file.

Deleting JMB Errors

To delete an error JMB:

1. From the Service Now task ribbon, select **Service Central > Incidents > JMB Errors**.

The **Manage JMB Errors** page is displayed.

2. Select the JMB that you want to delete.
3. Click **Delete** from the Actions panel.

The **Delete Error JMB** dialog box prompts you to confirm the deletion.

4. Click **Delete**.

The selected error JMBs are deleted from the Service Now database and they no longer appear on the **Manage JMB Errors** page.

- Related Topics**
- Service Central Overview on page 1
 - Messages Overview on page 13

CHAPTER 5

Notifications

- Notification Policies Overview on page 23
- Creating and Editing a Notification Policy on page 24
- Enabling or Disabling a Notification Policy on page 28
- Deleting a Notification Policy on page 29

Notification Policies Overview

In Service Now, a notification policy specifies the events for which you want Service Now to send a notification and also for 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 **Manage Notifications** page displays the notification policies chronologically by name, owner, status, and trigger. For more information about the Manage Notifications table columns, see Table 1 on page 23.

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	Not applicable.
Owner	Name of the user who owns the notification policy.	Not applicable.	Not applicable.	Not applicable.

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

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Status	Whether the notification policy is running.	Not applicable.	Enabled or Disabled	Not applicable.
Trigger Type	Type of the trigger for which the notification policy is applied.	Not applicable.	<ul style="list-style-type: none"> • New Incident Detected • Incident Submitted • Case ID Assigned • Case Status Updated • New Intelligence Update 	Not applicable.

- Related Topics**
- [Creating and Editing a Notification Policy on page 24](#)
 - [Enabling or Disabling a Notification Policy on page 28](#)
 - [Deleting a Notification Policy on page 29](#)

Creating and Editing a Notification Policy

Notification policies specify when you want Service Now to send notifications, and also who to send the notifications to. You can define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now must to 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 **Service Central: Create Notifications** page is displayed.

2. Enter a notification policy name and select a trigger.
3. Enter the filter parameters.
Different filters are supported for incident and information trigger types.
4. Enter the e-mail IDs of users to whom the notification must be sent.

For more information about the fields in the **Create Notification Policy** dialog box, see Table 2 on page 26.

5. Click **Add**.

The notification policy is created and displayed on the **Manage Notifications** page.

Copying a notification policy

You can also copy an existing notification policy and modify its attributes to create another notification policy.



NOTE: While copying a notification policy, you cannot edit the **Trigger** field.

To copy a notification policy:

1. From the Service Now task ribbon, select **Service Central > Notifications**.
The **Manage Notifications** page is displayed.
2. Select the notification policy that you want to copy.
3. Click **Copy** from the Actions panel.
The **Service Central: Notifications** page is displayed.
4. Make your modifications.
5. Click **Make a Copy**.

A notification policy is created with the settings that you specified.

Editing a 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. 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 26, and for more information see Table 3 on page 28.

Table 2: Create Notification Policy Page Field Descriptions

Field	Description	Range/Length	Default
Name	Enter the name of the policy, which must be unique to the policies a user owns.	64 characters	Not applicable.
Trigger Type	Enter the 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 Intelligence Update 	Not applicable.
Apply Filters:			
Common Filter Parameters:			
Priority	Select a value in the Priority field. Service Now sends a notification if the priority of the incident matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank

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

Field	Description	Range/Length	Default
Device Name	Enter a value in the Device Name field. Service Now sends 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 sends 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 sends 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
Does not have	Enter a value in the Doesn't have field. Service Now sends 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:			
Intelligence Update Type	Enter a value in the Intelligence Update Type field. Service Now sends 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 sends a notification if the Products Affected field value in alert information messages matches the entered value	255 characters	Blank
Platform Type	Enter a value in the Platform Type field. Service Now sends 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 sends a notification if the Keyword in information messages matches the entered value	255 characters	Blank
Serial Number	Enter a value in the Serial Number field. Service Now sends 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
Software Version	Enter a value in the Software Version field. Service Now sends a notification if the software version in the information messages matches the entered value	255 characters	Blank
Devices Impacted	Enter a value in the Devices Impacted field. Service Now sends a notification if the devices impacted in the information messages matches the entered value	255 characters	Blank
Has the words	Enter a value in the Has the words field. Service Now sends 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
Does not have	Enter a value in the Doesn't have field. Service Now sends 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

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

Field	Description	Range/Length	Default
Actions:			
Send Email to	Specify the e-mail addresses of users who must receive an alert if the policy is triggered and matches the specified filter. 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	Blank
Send Traps to	Specify the destinations where SNMP traps can be sent when an event occurs and matches the specified filter. See Adding an SNMP Server	Not applicable.	Not applicable.

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	Changes the status of the selected policies from Enabled to Disabled or vice versa

- Related Topics**
- Notification Policies Overview on page 23
 - Enabling or Disabling a Notification Policy on page 28

Enabling or Disabling a Notification Policy

Notification policies specify the events for which Service Now sends notifications, and the actions that Service Now takes in response to these events. They define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

To enable a notification policy:

1. From the Service Now task ribbon, select **Service Central > Notifications**.

The **Manage Notifications** page is displayed.

2. Select the notification policies whose status you want to change.
3. Click **Enable/Disable** from the Actions panel.

The **Change Reaction Policy Status** dialog box displays the name and status of the selected incident.

4. Click **Change Status** 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 23
 - Creating and Editing a Notification Policy on page 24

Deleting a Notification Policy

A notification policy specifies the events for which Service Now sends notifications, and the actions that Service Now takes in response to these events. It defines the events that trigger the notification, the filters that further specified the trigger events, and the actions that you want Service Now to take after the event is triggered.

To delete a notification policy:

1. From the Service Now task ribbon, select **Service Central > Notifications**.

The **Manage Notifications** page is displayed.

2. From the Notifications table, select the notification policy (or policies) that you want to delete.
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 23
 - Enabling or Disabling a Notification Policy on page 28

CHAPTER 6

Index

- Index on page 33

Index

D

deleting	
iJMB.....	18
incident.....	7
information message.....	15
notification policy.....	29

E

export iJMB	
html.....	17

I

incident	
assigning owner.....	4
export to HTML/excel.....	6
flagging.....	5
submitting.....	8
information message	
assign owner.....	14
flagging.....	14

J

JMB error.....	21
----------------	----

M

modify submit case options.....	10
---------------------------------	----

N

notification policy	
create.....	24
enable/disable.....	28

O

overview	
device snapshots.....	17
Incidents.....	3
messages.....	13
notifications.....	23
Service Central	1

S

scan iJMB for ipact.....	15
--------------------------	----

V

view	
case in case manager.....	9
iJMB details.....	18
incident details	8

