



Junos Space Service Now User Guide



Modified: 2016-06-23

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

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

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.

Junos Space Service Now User Guide

Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xiv
Chapter 1	Junos Space Service Now Overview	17
	Junos Space Service Now Overview	17
	Junos Space Service Now Modes	20
	Service Now MIBs	23
	Service Now Domain	24
	Assigning a Service Now Object to Another Domain	26
	Filtering Inventory Pages on Service Now and Service Insight	27
	Service Now Dashboard Overview	29
	Service Now Workspaces	29
	Dashboard Gadgets	30
	Platforms with Most Incidents	31
	Devices with the Most Incidents	31
	Service Now Notices (Upgrade and Contract Notice)	32
	Service Central Overview	32
Chapter 2	Service Now Getting Started Assistant	35
	Service Now Getting Started Assistant Usage Overview	35
Chapter 3	Managing Incidents	37
	Incidents Overview	37
	Viewing Incident Details	40
	Viewing Knowledge Base Articles Associated with an Incident	42
	Assigning an Owner to an Incident	42
	Submitting an Incident to Juniper Support Systems	44
	Flagging an Incident to a User	48
	Viewing a Case in Case Manager	49
	Exporting a Juniper Message Bundle (JMB) to an HTML file	50
	Updating an End-Customer Case	52
	Uploading an Attachment to an Incident	53
	Uploading Core Files to JSS for an Incident	55
	Checking Incident Status Updates	55
	Deleting an Incident	56

Chapter 4	Managing Cases	59
	Technical and End Customer Support Cases Overview	59
	Updating an End-Customer Case	62
	Uploading an Attachment to a Case	64
Chapter 5	Managing Messages	67
	Messages Overview	67
	Assigning Ownership to Messages	68
	Flagging a Message to Users	68
	Scanning a Message for Impact	69
	Assigning a Message to an End Customer	70
	Deleting a Message	72
Chapter 6	Managing Device Snapshots or iJMBs	73
	Device Snapshots Overview	73
	Viewing Details of a Device Snapshot	74
	Exporting Device Snapshots to HTML	76
	Deleting Device Snapshots	77
Chapter 7	Managing BIOS Validations	79
	BIOS Validation Overview	79
	Exporting BIOS Validation Results	82
	Deleting BIOS Validation Results	84
Chapter 8	Analyzing Physical Health Data	85
	Product Health Data Collection Overview	85
	Exporting Product Health Data Information to an Excel File	87
	Exporting Information about Devices on which PHDC is configured	88
	Exporting Data about PHD Files Collected from a Device	90
	Viewing Product Health Data Files Collected from a Device	92
	Deleting Product Health Data Files Collected from a Device	95
Chapter 9	Managing JMB with Errors	99
	JMBs with Errors	99
	Downloading JMBs with Errors	99
	Deleting JMBs with Errors	100
Chapter 10	Managing Notifications	101
	Notification Policies Overview	101
	Creating and Editing a Notification Policy	103
	Enabling or Disabling a Notification Policy	111
	Deleting a Notification Policy	111
Chapter 11	Trouble Ticketing	113
	Setting up Java Based Web Service Client	113
	Accessing a Web Service	118
Chapter 12	Trouble Ticket API	121
	Trouble Ticket APIs Overview	121
	Profiles Used by Service Now	122
	Trouble Ticket APIs Supported by Service Now	122
	Trouble Ticket Attributes Supported by Service Now	124

	Trouble Ticket Events Supported by Service Now	125
	Error Messages Displayed by OSS/J Client	127
Chapter 13	Index	131
	Index	133

List of Figures

Chapter 1	Junos Space Service Now Overview	17
	Figure 1: Service Now Operating in Direct Mode	21
	Figure 2: Service Now Operating in Partner Proxy and End Customer Modes	22
	Figure 3: Platform with Most Incidents Gadget	31
	Figure 4: Devices with Most Incidents Gadget	32
	Figure 5: Service Central Gadgets	33
Chapter 3	Managing Incidents	37
	Figure 6: Incident Detail Page	41
	Figure 7: Submit Case Options Page	45
	Figure 8: Export JMB to HTML Dialog Box	51
	Figure 9: End-Customer Cases Dialog Box	52
	Figure 10: Upload Attachment Dialog Box	54
Chapter 4	Managing Cases	59
	Figure 11: View Tech Support Cases	59
	Figure 12: View End Customer Cases Page	61
	Figure 13: End-Customer Cases Dialog Box	63
	Figure 14: Upload Attachment Dialog Box	64
Chapter 5	Managing Messages	67
	Figure 15: Choose Connected Members Dialog Box	71
Chapter 6	Managing Device Snapshots or iJMBs	73
	Figure 16: Juniper Message Bundle	75
	Figure 17: View JMB Dialog Box	76
Chapter 7	Managing BIOS Validations	79
	Figure 18: BIOS Validation Legal Notice on Service Now Partner	80
	Figure 19: BIOS Validation Legal Notice on Service Now End Customer	80
Chapter 8	Analyzing Physical Health Data	85
	Figure 20: Product Health Data Devices Page	86
	Figure 21: PHDC Information of Devices Exported to Excel	87
	Figure 22: PHD Files Information Exported to Excel	88
	Figure 23: View all Devices of this PHDC	89
	Figure 24: View All Product Health Data Files Page	91
	Figure 25: View All Devices of this PHDC Page	91
	Figure 26: View All Product Health Data Files Page	92
	Figure 27: View All Devices of this PHDC Page	94
	Figure 28: View All Product Health Data Files Page	96
	Figure 29: View All Devices of this PHDC Page	96

Chapter 9	Managing JMB with Errors	99
	Figure 30: Download JMB Errors Dialog Box	100
Chapter 10	Managing Notifications	101
	Figure 31: Create Notifications Page	104

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xii
	Table 2: Text and Syntax Conventions	xii
Chapter 1	Junos Space Service Now Overview	17
	Table 3: Features and Tasks Enabled for Service Now Modes	22
	Table 4: Service Now Objects and Their Default Domains	25
	Table 5: Filter-enabled Tables and Columns	27
	Table 6: Service Now Workspaces	30
Chapter 3	Managing Incidents	37
	Table 7: Fields on the Incidents Page	38
Chapter 4	Managing Cases	59
	Table 8: Fields on the View Tech Support Cases Page	60
	Table 9: Fields on the View End Customer Cases Page	61
Chapter 7	Managing BIOS Validations	79
	Table 10: BIOS Validations Field Descriptions	81
	Table 11: BIOS Validation Field Descriptions	82
Chapter 8	Analyzing Physical Health Data	85
	Table 12: Fields on the Product Health Data Devices Page	86
	Table 13: Fields on the View All Product Health Data Files Page	93
Chapter 10	Managing Notifications	101
	Table 14: Notification Triggers and Trigger Filters	101
	Table 15: Create Notification Policy Page Field Descriptions	105
Chapter 12	Trouble Ticket API	121
	Table 16: Trouble Ticket APIs Supported by Service Now	123
	Table 17: Supported Trouble Ticket Attributes	124
	Table 18: OSS/J Client Error Scenarios	127

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiv

Documentation and Release Notes

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

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

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

Supported Platforms

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

- JA1500
- JA2500
- Junos Space Virtual Appliance

Documentation Conventions

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

Table 1: Notice Icons







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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

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

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Junos Space Service Now Overview

- [Junos Space Service Now Overview on page 17](#)
- [Junos Space Service Now Modes on page 20](#)
- [Service Now MIBs on page 23](#)
- [Service Now Domain on page 24](#)
- [Filtering Inventory Pages on Service Now and Service Insight on page 27](#)
- [Service Now Dashboard Overview on page 29](#)
- [Service Central Overview on page 32](#)

Junos Space Service Now Overview

Junos Space Service Now is an application that runs on the Junos Space Network Management Platform to automate fault management and accelerate issue resolution. This application significantly reduces the resolution time by automating support processes and using device diagnostics for fault monitoring and case automation. Your contract with Juniper Networks determines whether Service Now operates in standalone mode, partner proxy mode, end customer mode, or offline mode. These modes in turn determine which tasks are enabled and disabled in Service Now. For information about Service Now modes, see *Service Now Modes*.

Service Now receives information about events, such as a process crash, an ASIC error, or a fan failure, when they occur on a device from AI-Scripts installed on the device. AI-Scripts detect an event on the device on which they are installed and automatically collect diagnostic data for the event and package the data into an XML file called *Juniper Message Bundle* (JMB).

AI-Scripts operate in the following modes to generate a JMB:

- **Reactive mode:** In reactive mode, the AI-Scripts collect data from the device when a predefined event, such as failure to allocate memory for a process or failure of a hardware, occurs on the device and store the data at a predefined location on the device from where Service Now accesses it for analysis and resolution. The JMB generated in this mode is known as an event JMB or eJMB.

An eJMB usually includes the device identity, the problem event, log files, and core files. This information is securely transferred to the Junos Space Platform. Service Now

creates an incident in response to the event and the received JMB. Service Now then notifies users about the new incident by sending an e-mail or an SNMP trap.

- Proactive mode: In proactive mode, the AI-Scripts periodically collect data on vital system functions and store the data at a predefined location on the device. This data is accessed by Service Now to monitor the device and to predict and prevent risks related to the device. The JMB generated in this mode is known as an informational JMB or iJMB.

Apart from event and informational JMBs, AI-Scripts also generate JMBs in response to an event triggered by a user. These JMBs are known as on-demand incident JMBs. When you submit an on-demand incident on the device by using Service Now, Service Now generates an on-demand incident JMB by executing preconfigured CLIs on the device.

Service Now categorizes the JMBs that do not comply with the defined standard data structure or that contain unexpected data elements as error JMBs. Service Now displays the error JMBs on the JMB Errors page. From the JMB Errors page, you can view and download the error JMBs.

In response to a JMB collected from a device, Service Now creates an incident and notifies users about the incident by sending an e-mail or an SNMP trap. You can submit the incident to Juniper Support Systems (JSS), after reviewing the information provided in the JMB, to create a Juniper Networks Technical Assistance Center (JTAC) case. You can also configure Service Now to submit an incident automatically to JSS as soon as the incident is created. Service Now provides an option to filter the device configuration information from a JMB before you share the information with JSS or a Service Now partner (if Service Now is operating in end customer mode).

JSS sends updates to Service Now for you to track the status of the case.

Apart from submitting JMBs to obtain resolutions, you can use Service Now to perform the following tasks:

- Assign an owner (user) to a reported incident.
- Keep users informed about changes made to the incident.
- Set up notification policies for users who need to be kept informed about changes to incidents that affect them.
- Update the incident status.
- Delete JMBs from the Service Now database.
- Export data in the incident and information messages to HTML or CSV format and store the data on the local file system.

To submit incidents, share JMBs, and open support cases with JSS, you must first configure an organization in Service Now. An organization represents a unique Clarify site ID in JSS that is used to identify customers while providing technical support. To add multiple organizations and devices to Service Now, you need to obtain a technical support contract with the level of service that you require. After you have a valid contract, you can submit incidents and iJMBs to JSS for support. Without a valid contract, Service Now runs in

demo mode and supports one organization and five devices for 60 days. In this mode, you cannot connect with JSS or open technical support cases with JTAC.

If you are a Juniper Networks partner or a direct customer with multiple distinct networks, you can use multiple Service Now organizations to keep customers or networks separate.

For Service Now to monitor and detect events on devices, you must discover the devices by using the Junos Space Network Management Platform, add the devices to Service Now, and then install AI-Scripts on the devices. You can categorize the devices into device groups to manage the devices as a single entity. For example, you can install or remove AI-Scripts simultaneously on all devices in a device group. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses.

Service Now also sends SNMP traps if notification policies are configured to send traps when events occur on devices. From Service Now Release 14.1 and Service Insight Release 14.1, Service Now and Service Insight use proxy server configured on the Junos Space Platform to facilitate all communication over the Internet.

The Service Now dashboard displays the gadgets and workspaces that the user can use to perform various tasks. For more information about the Service Now dashboard, see [“Service Now Dashboard Overview” on page 29](#).

From the Release 14.1 of Junos Space Platform, Service Now, and Service Insight, Service Now and Service Insight are available as hot-pluggable applications. This makes it possible for you to install, upgrade, and uninstall Service Now and Service Insight applications independently of the Junos Space Platform. See the *installing, Upgrading, and Uninstalling Junos Space Service Now* section of the *Service Automation Quick Start Guide* for information about installing, upgrading, and uninstalling Service Now and Service Insight.

To install, upgrade, and uninstall Service Now from a Junos Space server, you need Junos Space administrator privileges. You can install, remove, or upgrade Service Now even while Junos Space and Junos Space applications are still running. Refer to *Junos Space Service Now User Roles* for information about user roles and tasks that can be performed for a user role.

**Related
Documentation**

- [Service Central Overview on page 32](#)
- *Administration Overview*
- [Service Now Domain on page 24](#)
- *Insight Central Overview*

Junos Space Service Now Modes

Junos Space Service Now collects event and trending data (in the form of Juniper Message Bundles [JMBs]) from devices running Junos OS and submits the data to Juniper Support System (JSS) for troubleshooting and analysis. JSS identifies the Service Now application by the organization configured on it. An organization is configured on Service Now with a unique site ID and credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks or a qualified Juniper Networks partner (when Service Now is operating in End Customer mode).

Service Now periodically checks and collects JMBs from the managed devices and creates an incident for each JMB collected from the devices. A user can submit an incident manually or configure Service Now to submit an incident automatically to JSS for creating a case. A case is created in JSS and associated with the site ID of the organization configured on Service Now from which the incident was submitted.

Depending on your contract with Juniper Networks, you can operate Service Now in Direct, End Customer, or Partner Proxy modes. Certain features are enabled or disabled depending on the mode of operation.

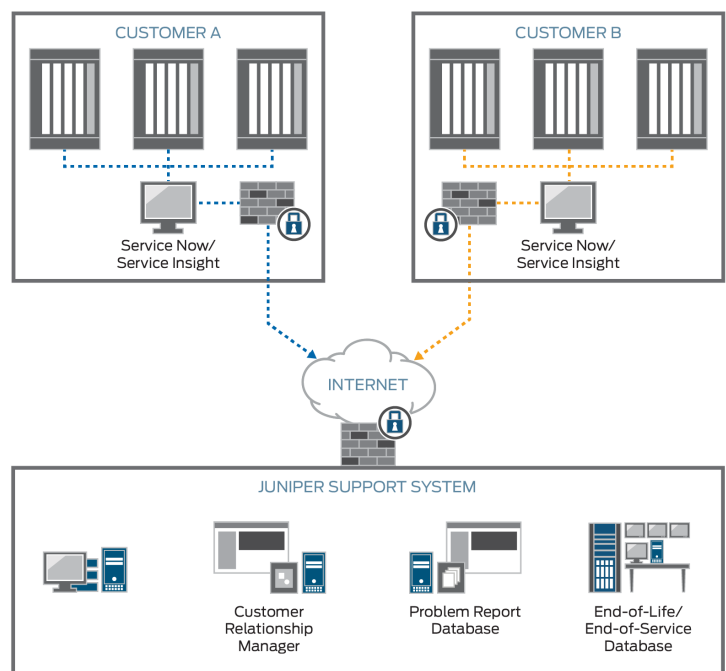
- Demo mode—Service Now operates in Demo mode from the time you install Service Now on Junos Space Network Management Platform until you create an organization and validate the organization by establishing a connection with JSS or a Service Now partner.

In Demo mode, you can add one organization and up to five devices, manage device inventory, install AI-Scripts on the devices, detect events on the devices, and view JMBs collected from the devices.

- Offline mode—You can accept a Direct or Partner Proxy license file and activate the Junos Space Platform and Service Now application without having to connect to JSS. You can perform all Service Now tasks except submit incidents, create autosubmit policies, view exposures, or view cases in Case Manager. If Service Now is already in End Customer mode, you cannot operate it in Offline mode.
- Direct mode—In Direct mode, you can add multiple Service Now organizations and devices in Service Now. Service Now is connected to JSS, which enables you to submit incidents to JSS and JSS to provide support for the incidents that you submit.

[Figure 1 on page 21](#) shows Service Now operating in Direct mode.

Figure 1: Service Now Operating in Direct Mode



- **Partner Proxy mode**—A qualified Juniper Networks partner (also known as Service Now partner) can operate Service Now in Partner Proxy mode to manage multiple Service Now end customers (also known as connected members). The Service Now end customers submit incidents to the Service Now partner, who resolves the issues or submits the issues to JSS for resolution.

You can configure multiple organizations and end customers and manage multiple devices in this mode.

- **End Customer mode**—In End Customer mode, Service Now communicates with JSS through the Service Now partner. When events occur on the devices managed by an end customer, incidents are reported to the Service Now partner. The Service Now partner, if required, submits the incidents to JSS for resolution. The Service Now partner provides the required credentials to an end customer for configuring the Service Now organization.

You can configure only one organization, but can manage multiple devices in this mode. [Figure 2 on page 22](#) shows Service Now operating in Partner Proxy and End Customer modes.

Figure 2: Service Now Operating in Partner Proxy and End Customer Modes

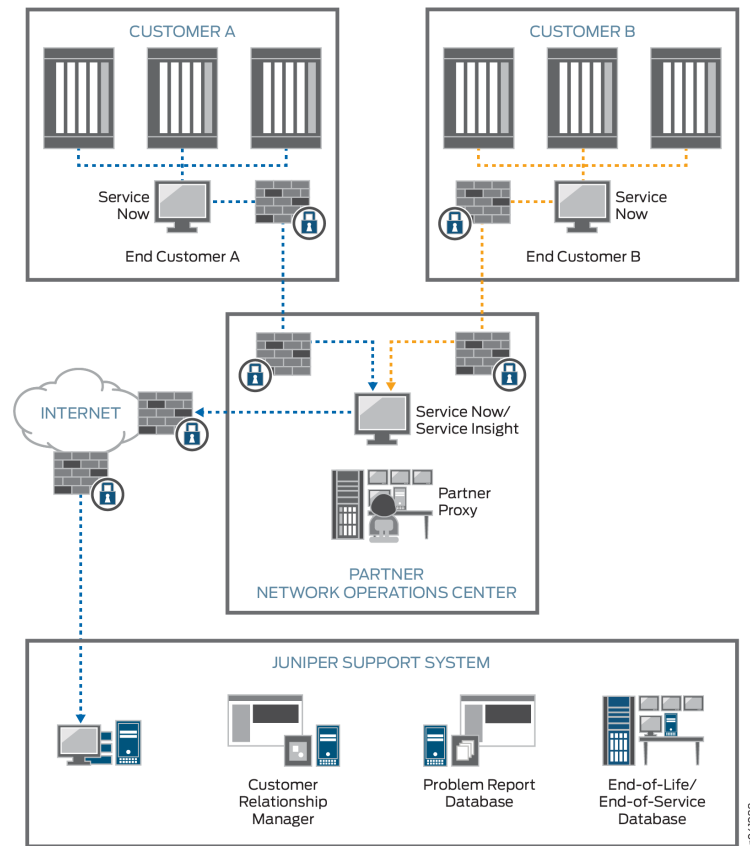


Table 3 on page 22 highlights some of the differences among the various modes of operating Service Now.

Table 3: Features and Tasks Enabled for Service Now Modes

Task	Demo Mode	Offline Mode	Direct Mode	Partner Proxy Mode	End Customer Mode
Number of devices supported	5	Multiple	Multiple	Multiple	Multiple
Number of organizations supported	1	Multiple	Multiple	Multiple	1
Adding connected members	–	–	–	Enabled	–
Updating end-customer cases	–	–	–	Enabled	–

Table 3: Features and Tasks Enabled for Service Now Modes (*continued*)

Task	Demo Mode	Offline Mode	Direct Mode	Partner Proxy Mode	End Customer Mode
Assigning messages to an end - customer	–	–	–	Enabled	–
Viewing messages assigned to an end - customer	–	–	–	Enabled	–
Submitting incidents for creating technical support cases to JSS	Disabled	–	Enabled	Enabled	Disabled (but can submit incidents to the Service Now partner)
Installing or removing AI-Scripts on or from devices	Enabled	Enabled	Enabled	Enabled (only for devices managed directly by the Service Now partner)	Enabled
Validating the BIOS	Disabled	–	Enabled	Enabled	Enabled
Product Health Data Collection	–	–	Enabled	Enabled	–
Other tasks (viewing incidents, configuring notifications, receiving JMBs, managing the inventory, and so on)	Enabled	Enabled	Enabled	Enabled	Enabled

Related Documentation

- [Administration Overview](#)
- [Service Central Overview on page 32](#)
- [Configuring Global Settings](#)
- [Adding an Organization to Service Now](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode](#)

Service Now MIBs

Service Now supports Juniper Networks enterprise-specific management information bases (MIBs). These MIBs define the traps that Service Now sends to a remote network management system. The sent traps correspond to the trigger specified for a notification

policy. For information about creating a notification policy in Service Now, see [“Creating and Editing a Notification Policy” on page 103](#).

Using Service Now notifications, you can configure Service Now to send SNMP traps to one or more of your SNMP servers. To enable an SNMP server to receive traps from Service Now, load the following MIBs in the order listed below:

1. jnx-smi.mib
2. jnx-ai-manager.mib

To download these MIB files:

- From the Application Chooser, select **Service Now**. The dashboard appears, which displays the **Service Now Notices** box.
- In the **Service Now Notices** box, click the **click here** link provided in the **To download Service Now Mibs click here** statement.

The **Technical Documentation** page opens. The Service Now MIBs are stored by release versions in this page.

- Click the respective version to download the required MIB files.

Related Documentation

- [Adding an SNMP Configuration to Service Now](#)
- [Junos Space Service Now Overview on page 17](#)
- [Service Now MIBs Downloads](#)

Service Now Domain

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

A device is assigned to a domain in the Junos Space Network Management Platform. When the device is added to Service Now, the device continues to belong to the domain to which it is assigned in the Junos Space Network Management Platform. Service Now objects such as incidents, device snapshots, error JMBs, and support cases that are related to the device are assigned to the same domain as the device.

When you log in to Service Now, objects such as organization, script bundle, SNMP configuration, and Email template, which are assigned to the domain that you are currently in, and the objects in the system domain are visible to you. If you are assigned to more than one domain, you can access the other domains and objects in those domains by selecting the domains from the **Login as username in** list. Only the domains to which you are assigned are listed. A super user can access all domains.

Objects that you create when you are logged in to a certain domain are assigned to that domain. However, if you have administrative privileges, you can assign the objects to

another domain. For information about changing the domain of an object, refer to [“Assigning a Service Now Object to Another Domain” on page 26](#).

Objects such as script bundles, SNMP configurations, and Email templates that are used by objects in all domains are assigned to the system domain. Objects assigned to the system domain are visible in all domains.

You cannot modify the domain of Service Now devices and the objects such as incidents, error JMBs, device snapshots, and support cases related to the Service Now devices. However, you can modify the domain of devices of end customers. The devices of end customers are, by default, present in the domain assigned to them by the connected member.

When the device is assigned to a domain, objects such as technical or end-customer support cases that are not assigned to any device belong to the domain assigned to the organization associated with the device. [Table 4 on page 25](#) lists Service Now objects and their default domains.

Table 4: Service Now Objects and Their Default Domains

Service Now Objects	Default Domain	
	Fresh Installation	Migration
<ul style="list-style-type: none"> • Organization • Connected Member • Device Group • Address Group • Notification • Auto Submit Policy • Event Profile • Product Health Data Configuration 	Domain to which a user is logged in	Global domain
<ul style="list-style-type: none"> • Global Setting • SNMP Configuration • Core File Upload Configuration • Message • Script Bundle • Email Template • End Customer Information Message • Script Installation Advisor (SIA) 	System domain	System domain

Table 4: Service Now Objects and Their Default Domains (*continued*)

Service Now Objects	Default Domain	
	Fresh Installation	Migration
<ul style="list-style-type: none"> • Service Now Device • Incident • Device Snapshot • Error JMB • Technical Support Case • End Customer Case 	Domain assigned to the device in Junos Space Network Management Platform	Domain assigned to the device in Junos Space Network Management Platform

Assigning a Service Now Object to Another Domain

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

To assign a Service Now object to another domain:

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

The object's landing page appears.

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

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

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

The Assign to Domain dialog box appears.

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

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

5. From the **Login as username** in list, select the domain to which you assigned the object.

The Service Now GUI is refreshed.

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

Related Documentation

- [Service Central Overview on page 32](#)
- [Administration Overview](#)
- [Domains Overview](#)

Filtering Inventory Pages on Service Now and Service Insight

All the inventory pages provide column based filtering so that you can filter data by a specific column. The filters are present in the drop-down list of the columns. The drop-down list has an input field where you can enter the filter criteria. On applying the filters, the table contents display values that match the applied filter criteria.

Depending on the table, different columns can be filtered on. [Table 5 on page 27](#) lists the tables that permit filtering.

Table 5: Filter-enabled Tables and Columns

Work-space	Page / Table	Columns
Administration	Organizations	All columns except: <ul style="list-style-type: none"> • Submit Cases As
	Device Groups	All columns
	Service Now Devices	All columns except: <ul style="list-style-type: none"> • Connected Member • Ship-to • Location • Policy
	Event Profiles	All columns except: <ul style="list-style-type: none"> • Devices
	Script Bundles	All columns
	Product Health Data Collection	All columns except Devices
	Auto Submit Policy	All columns except: <ul style="list-style-type: none"> • Events • Devices • Incident Submitted
	Address Group	All columns except: <ul style="list-style-type: none"> • Devices
	E-mail Templates	All columns except: <ul style="list-style-type: none"> • Description

Table 5: Filter-enabled Tables and Columns *(continued)*

Work-space	Page / Table	Columns
Service Central	Incidents	All columns except: <ul style="list-style-type: none"> • Connected Member • Total Core Files • Flag
	View Tech Support Cases	All columns except: <ul style="list-style-type: none"> • Organization • Time Created
	View End Customer Cases	All columns
	Information messages	All columns except: <ul style="list-style-type: none"> • Organization
	BIOS Validations	All columns except: <ul style="list-style-type: none"> • Connected Member (in Partner Proxy mode) • Junos Version
	Product Health Data Devices	All columns except View.
	Device Snapshots	All columns except: <ul style="list-style-type: none"> • Connected member
	JMB Errors	All columns
	Notifications	All columns
Insight Central	Exposure Analyzer	All columns except: <ul style="list-style-type: none"> • Connected Member
	EOL Reports	All columns except: <ul style="list-style-type: none"> • Devices selected
	PBN Reports	All columns except: <ul style="list-style-type: none"> • Devices selected
	Targeted PBNs	All columns
	Notifications	All columns

For procedure regarding filtering inventory pages, see *Filtering Inventory Pages* section from the *Junos Space Network Management Platform User Guide*.

- Related Documentation**
- [Service Central Workspace Overview on page 32](#)
 - [Service Insight Workspaces](#)

Service Now Dashboard Overview

The Service Now dashboard displays notifications and graphs about platforms and devices with most incidents. You can view the Service Now dashboard by selecting **Service Now** from the Application Chooser.

The Service Now dashboard includes:

- [Service Now Workspaces on page 29](#)
- [Dashboard Gadgets on page 30](#)

Service Now Workspaces

Apart from the Service Central and Administration workspaces, Service Now also provides shortcuts to the Devices and Jobs workspaces by including them in the Service Now navigation tree.

For more details, refer to *Junos Space Network Management Platform User Guide*.

You can perform the following tasks from the **Jobs** workspace:

- View status of all scheduled, running, canceled, and completed jobs
- Retrieve details about the execution of a specific job
- View statistics about the average execution times for jobs, types of jobs that are run, and success rate
- Cancel a scheduled job or in-progress job when the job is stalled and is preventing other jobs from starting
- Archive old jobs and purge them from the Junos Space Network Management Platform database
- Retry a job on failed devices on Service Now and Service Insight. The action **Retry on Failed Devices** is available for the following jobs:
 - Failed event profile installation
 - Failed event profile un-install
 - Failed create on-demand incident job

For retrying jobs on failed devices, see [Retrying a Job on Failed Devices](#) from the *Junos Space Network Management Platform user Guide*.

[Table 6 on page 30](#) lists the tasks that can be performed using the Service Now workspaces.

Table 6: Service Now Workspaces

Workspace Name	Tasks
Service Central	<ul style="list-style-type: none"> Assign an incident to a user to take the ownership, notify users about the incident, update the status of incidents, and delete incidents. View and delete JMBs, and export device data into HTML format. Deliver messages from JSS to customers (enabled if you are a Juniper Networks partner and working in partner-proxy mode). Update customer cases (enabled if you are a Juniper Networks partner and working in partner-proxy mode). View devices from which BIOS data is collected and the time BIOS data was collected. View devices from which product health data is collected and the product health data files collected from the devices. View, download, and delete JMBs with errors from the Service Now database. View Knowledge Base (KB) articles associated with incidents. View information about devices that risk the chance of exposure. Assign an owner, flag to users, and delete an information message. Create, edit, and delete a notification policy.
Administration	<ul style="list-style-type: none"> Add devices to Service Now from the Junos Space platform. Add or delete an event profile or a script bundle. Add and delete devices and device groups. Install or remove AI-Scripts on devices. Associate devices with device groups. Add, modify, or delete an organization. Add connected members and view messages assigned to them (enabled if you are a Juniper Networks partner and working in partner-proxy mode). Create organizations in test mode and test the connectivity between the organization and JSS. Export device data in CSV and Excel formats. Configure product health data collection on devices. Export inventory information in CSV format. Configure the global settings (SNMP server and core file upload). A client can associate address location to devices, and a user can associate a device location or a ship-to-address to a device. Modify E-mail templates.

Dashboard Gadgets

The Service Now dashboard displays gadgets (graphs and charts) with information that is updated automatically. You can move the gadgets on the dashboard and change their

sizes. These changes persist even after you log out of the system. The gadgets displayed on the Service Now dashboard are:

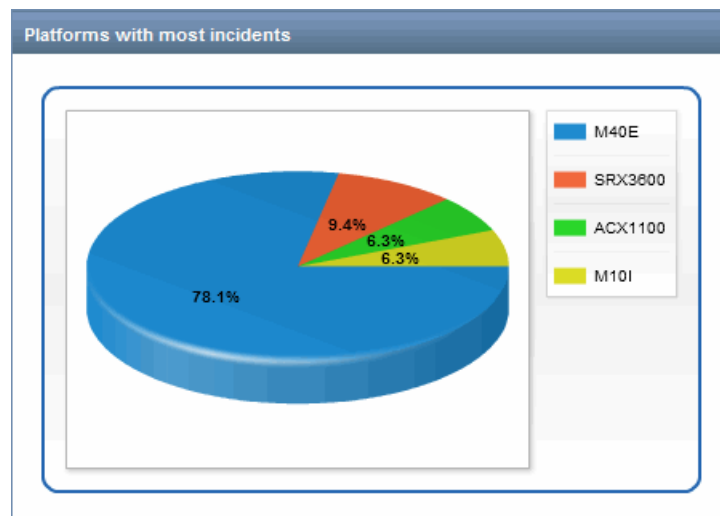
- [Platforms with Most Incidents on page 31](#)
- [Devices with the Most Incidents on page 31](#)
- [Service Now Notices \(Upgrade and Contract Notice\) on page 32](#)

Platforms with Most Incidents

This gadget graphically displays the platforms with the most incidents and the percentage of incidents detected on them. Clicking the elements within the graph takes you to the Incidents page, where incidents are filtered to display only the incidents that occurred on the platform that you clicked.

For example, when you click the **ACX1100** element in the **Platforms with most incidents** gadget (as shown in [Figure 3 on page 31](#)), the Incidents page displays only those incidents that are detected on the ACX1100 router.

Figure 3: Platform with Most Incidents Gadget

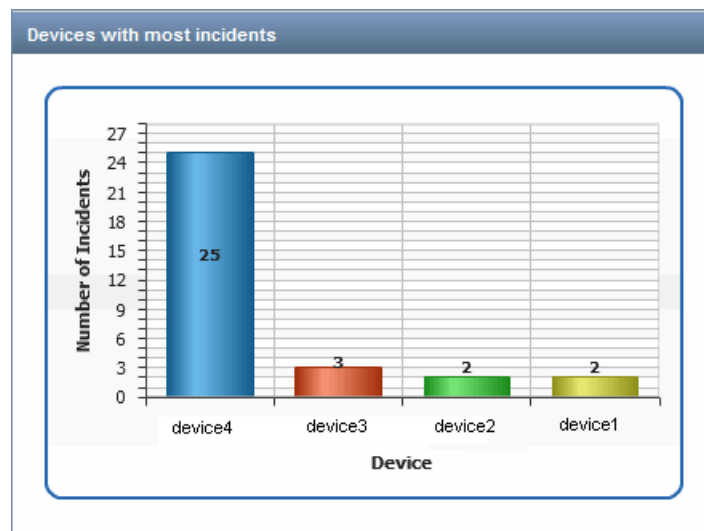


Devices with the Most Incidents

This gadget displays the devices with the most incidents graphically, along with the number of incidents detected on them. Clicking the elements within the graph takes you to the Incidents page, where incidents are filtered by the device category. You see only the incidents that affect the device that you selected. You can filter the incidents on the Manage Incidents page according to your selection on this graph. To do this, click the **Devices** bar of your choice in the graph to take you to the Manage Incidents page, which displays only those incidents that affect the device that you selected.

As shown in [Figure 4 on page 32](#), clicking **device1**, which is represented by the yellow bar of the graph, displays the Incidents page where incidents are filtered to display only those incidents that occurred on device1.

Figure 4: Devices with Most Incidents Gadget



Service Now Notices (Upgrade and Contract Notice)

This gadget notifies you about the tasks that you need to execute after a Junos Space upgrade. It also informs you about your contract with Juniper Networks.

- Related Documentation**
- [Service Central Overview on page 32](#)
 - [Administration Overview](#)

Service Central Overview

The Service Central workspace enables you to manage incidents, information messages, device snapshots, notifications, and error JMBs. 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 Incidents page within Service Central.

The Service Central workspace provides the following three gadgets:

- Incident severities—provides a graphical representation of the incidents generated and their severity.
- Incident priorities—provides a graphical representation of the incidents generated and their severity.
- My Incidents—provides a graphical representation of the incidents created new, flagged to you, or owned and changed by you.

Clicking the bar on the graph takes you to the respective incidents.

Figure 5: Service Central Gadgets



After viewing an incident, you can use the Incidents menu on the Service Now navigation tree to submit a case to the Juniper Support Systems (JSS). You can also notify other users about the incident, assign a user as an owner of the incident, and delete the incident from the device.

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 Device Snapshots page. You can upload these iJMBs to JSS, where they are processed and analyzed to provide preventive analysis and alerts. You can view the content of these iJMBs and export them to HTML format.

In certain cases, when devices stop sending device information, Service Now generates the iJMBs for all the devices associated to a device group. These iJMBs are generated based on the commands available in directive file pre-loaded in Service Now. The content of these iJMBs is the same as AI-Scripts generated iJMBs. Service Now administrator receives a message when Service Now generates iJMBs automatically for one or more devices.

A JMB is considered erroneous if it does not comply with the standard data structure that Service Now requires or if it contains data elements that Service Now does not accept. Service Now identifies these JMBs and displays them on the JMB Errors page from where they can be viewed and downloaded.

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 within the Service Central workspace, such as assigning messages to a connected member and updating an end-customer case, are enabled only when Service Now operates in the end-customer mode. For more information about 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 a user to own and manage incidents, notify users about the incidents, update the status of the incidents, and delete incidents.
- View and delete iJMBs, and export device data to HTML format.
- View devices from which BIOS data is collected and the time BIOS data was collected.
- View devices from which product health data is collected and the product health data files collected from the devices.
- Assign messages to end-customers (enabled if Service Now is operating in the partner-proxy mode).
- Update customer cases (enabled if Service Now is operating in the partner-proxy mode).
- View, download, and delete JMBs with errors.
- View Knowledge Base articles associated with incidents.
- View information about devices that are susceptible to known issues.
- Assign an owner, flag to users, and delete an information message.
- Create, edit, and delete a notification policy.

**Related
Documentation**

- [Junos Space Service Now Overview on page 17](#)
- [Service Now Modes](#)
- [Incidents Overview on page 37](#)
- [Device Snapshots Overview on page 73](#)
- [Messages Overview on page 67](#)
- [JMBs with Errors on page 99](#)
- [Notification Policies Overview on page 101](#)
- [Technical and End Customer Support Cases Overview on page 59](#)

CHAPTER 2

Service Now Getting Started Assistant

- [Service Now Getting Started Assistant Usage Overview on page 35](#)

Service Now Getting Started Assistant Usage Overview

The Getting Started assistant is a sections in the Junos Space sidebar that guides you through the tasks that you can perform as part of the initial setup for every application. It appears when you log in to Junos Space and the **Show Getting Started on Startup** check box is selected.

To use the Service Now Getting Started assistant, navigate to Service Now, click the **Help** icon, expand the **Getting Started** assistant, and click the **Initial Setup** link. The **Getting Started** assistant displays five required steps and one optional step.

Every step in the Getting Started assistant contains a task link, and alongside the task links are help icons that provide information about the individual tasks. To execute the steps, click the task links of every step. The inventory page displays the page where you can execute the tasks.

By default, the Getting Started assistant guides you through the steps required to set up Direct mode for Service Now.

The following steps are required:

1. Review Global Settings.
See [Configuring Global Settings](#).
2. Create an Organization.
See [Adding an Organization to Service Now](#).
3. Add Devices to Junos Space.
*See the [Discovering Devices](#) section of the *Junos Space Network Management Platform User Guide*.*
4. Create a Device Group.
See [Creating a Device Group](#).
5. Install Scripts using Service Now Devices.
See [Installing an Event Profile on a Device by Using Service Now](#).

The following step is optional:

- Add a New Script Bundle.
See *Adding a Script Bundle to Junos Space Service Now*.

To activate Service Now in end-customer and partner-proxy modes, see the Activating the End-Customer and Partner-Proxy Modes section in *Service Now Modes*.

**Related
Documentation**

- [Junos Space Service Now Overview on page 17](#)

CHAPTER 3

Managing Incidents

- [Incidents Overview on page 37](#)
- [Viewing Incident Details on page 40](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Flagging an Incident to a User on page 48](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Updating an End-Customer Case on page 52](#)
- [Uploading an Attachment to an Incident on page 53](#)
- [Uploading Core Files to JSS for an Incident on page 55](#)
- [Checking Incident Status Updates on page 55](#)
- [Deleting an Incident on page 56](#)

Incidents Overview

An incident is the occurrence of a defined event in a device. When an event, such as a process crash, an application-specific integrated circuit (ASIC) error, or a fan failure occurs on an AI-Scripts-enabled device, the AI-Scripts builds a Juniper Message Bundles (JMBs) file with the event data which is accessed by Junos Space Service Now.

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. The JMB file contains information such as hostname, time stamp of the event, synopsis, description, chassis serial number of the device, and the severity and priority of the event. After a JMB is generated, it is stored at a defined location in the device from where Service Now collects it. For each JMB collected, Service Now creates an incident. The incidents can be viewed on the incidents page.

Service Now uses Device Management Interface (DMI), which is an extension to the NETCONF network management protocol, to access JMBs from devices. The Incidents page provides a user interface to view incidents chronologically, by organization name, and by device group. The Quick 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 and Inventory Pages*.

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 can 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.

[Table 7 on page 38](#) lists the fields on the Incidents page.

Table 7: Fields on the Incidents Page

Fields	Description
Organization	The organization associated with the device for which the incident is created.
Device Group	The device group associated with the device for which the incident is created.
Priority	The priority of the incident.
Type	The type of defect.
Incident ID	The ID of the incident.
Incident Type	<p>The type of incident. This parameter can have one of the following values:</p> <ul style="list-style-type: none"> Event—indicates that an event is detected on the Service Now managed devices. On-demand—Indicates that the incident created is an on-demand incident. Event-RMA—indicates that an RMA event is detected on the Service Now managed devices. Event (low end)—indicates that the JMB generated on a device is a low impact JMB. User can manually collect troubleshooting data and update case through Case Manager or Service Now. On-demand RMA—Indicates that the RMA event detected on the device is an on-demand event. AIS Health Check—Indicates the incident is created in response to a JMB collected to obtain information about AI-Scripts error.
Device	The device on which the incident occurred.
Product	The hardware platform the device belongs to.
Occurred	The date and time the incident was created on Service Now.
Total Core Files	The number of core files available for the incident.
Status	The status of the incident.

Table 7: Fields on the Incidents Page (*continued*)

Fields	Description
Flagged	Specifies users are flagged to receive updates about the incident.

You can perform the following tasks from the Incidents page:

- Export JMB to HTML; see [“Exporting a Juniper Message Bundle \(JMB\) to an HTML file” on page 50](#) for details.
- Delete an incident; see [“Deleting an Incident” on page 56](#) for details.
- View JMBs.
- View a Knowledge Base (KB) article pertaining to the incident; see [“Viewing Knowledge Base Articles Associated with an Incident” on page 42](#) for details.

View a case in the Juniper Networks Case Manager; see [“Viewing a Case in Case Manager” on page 49](#) for details.

- Assign the incident to a user; see [“Assigning an Owner to an Incident” on page 42](#) for details.
- Flag an incident to a user; see [“Flagging an Incident to a User” on page 48](#) for details.
- Submit an incident to create a JTAC case; see [“Submitting an Incident to Juniper Support Systems” on page 44](#) for details.
- Export the summary of an incident to Excel; see for details.
- Updating an end customer case; see [“Updating an End-Customer Case” on page 52](#) for details.
- Create auto submit policy for an incident; see for details.
- Upload core files to JSS for incidents; see [“Uploading Core Files to JSS for an Incident” on page 55](#) for details.
- Upload attachments; see [“Uploading an Attachment to an Incident” on page 53](#) for details.



NOTE: Junos OS devices may not provide specific time zones for incidents, and hence Service Now may display an incorrect time of occurrence for incidents. For example, when the time zone is EST, Service Now uses US EST by default, while the time zone can also be AEST (Australian EST).

Related Documentation

- [Checking Incident Status Updates on page 55](#)
- [Viewing Incident Details on page 40](#)
- [AI-Scripts Overview](#)
- [Service Now Modes](#)
- [Auto Submit Policy Overview](#)

- [Junos Space Service Now Devices Overview](#)
- [Notification Policies Overview on page 101](#)

Viewing Incident Details

An incident is generated in Service Now when an event occurs on a device running Junos OS. An incident includes the following information:

- **Incident details:** Provides information about the event for which the incident is created—the device on which the event occurred, IP address of the device, the Junos OS version installed on the device, the time of the event, the link to the Knowledge Base for the event, and so on.
- **Case details:** Provides information about the case generated in Juniper Support Systems (JSS) for the incident—the case ID, site ID, synopsis of the incident, whether the incident was auto submitted to JSS; if auto submitted, the auto submit policy used to auto submit, filter level defined for sharing information with JSS and so on.
- **Core file details:** Provides information about the core files generated for the event—the path to the core file on the device, the size of the core file in bytes, the time the core file was generated, whether the core file is uploaded to JSS and deleted from the device after copying it to Service Now.



NOTE: For an end customer Service Now, core files are uploaded to the Service Now partner instead of JSS. The core files are uploaded to JSS from Service Now partner.

- **Attachment details:** Provides information about the attachments generated for the event—the path to the attachment files on the device, the size of the attachment file in bytes, the command used to generate the attachment file, whether the attachment is copied to Service Now and uploaded to JSS.
- **Log file details:** Provides information about the log files generated for the event—the path to the log file on the device, the size of the log file in bytes, whether the log file is copied to Service Now and uploaded to JSS.

To view incident details:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Double click on an incident to view its details. The **Incident Detail** page appears.



NOTE: If the selected incident type is Event (low end), the Problem Description field in the Incidents Detail page highlights the low end JMB with the note section that contains the following information: *This incident is based on a "low impact" JMB. A low impact JMB was generated to preserve system resources on the network node. Low impact JMBs do not include all the troubleshooting information found in a traditional JMB. A list of command output recommended for this event, but not contained in the low impact JMB, is listed below. If you open a case with this incident you can attach the recommended command output to the case by clicking the Incident and then the "view in case manager" action in Service Now.*

AI-Scripts adds this content when generating event based JMBs or eJMBs.

The **Incident Detail** page displays the following tabs: Incident Details, Case Details, Core File Details, Attachment Details, and Log File Details as shown in [Figure 6 on page 41](#). The **End-Customer Case Details** tab appears in the partner proxy mode for end customer incidents.

Figure 6: Incident Detail Page

The screenshot shows the 'Incident Detail' page with the following tabs: Incident Details (selected), Case Details, Core File Details, Attachment Details, and Log File Details. The main content area displays the following information:

- Device: device1
- IP Address: 192.0.100.0
- Device Serial Number:
- Product: EX-XRE
- Platform: junos-ex
- Release: 12.3R6
- Version: R6
- Organization: Test-Organization
- Device Group: Device Group for Test-Organization
- Occurred: Feb 11, 2014 2:15:51 PM IST
- Status: Submitted
- Incident ID: device1-999-2014011-004549-999
- Event Type: -
- Defect Type: -

At the bottom, there is a section for 'KB Article: None'.

You can retrieve required information from the tabs.

Related Documentation

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)

- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)
- *Troubleshooting Issues with Creating Incidents*

Viewing Knowledge Base Articles Associated with an Incident

Knowledge Base provides information about the causes and solutions for a problem. Using Service Now you can view Knowledge Base (KB) articles associated with an incident.

To view the KB article associated with an incident:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents table appears.
2. Select an incident to view the KB article associated with it, and select **View KB Article** from either the **Actions** list or the right-click menu.

A new window takes you to the Juniper Networks Knowledge Base article page where you can log in and view the KB article.



NOTE: This action is disabled for incidents that do not have any associated Knowledge Base (KB) articles.

Related Documentation

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)

Assigning an Owner to an Incident

You can assign a user to own and manage an incident. The owner tracks the progress of the related case and the updates from JSS.

To assign an incident to a Service Now user:

1. From the Service Now navigation tree, select **Service Central > Incidents**.

The Incidents page appears.

2. Select the incident to which you want to assign an owner, and select **Assign Ownership** from either the **Actions** list or the right-click menu.

The **Assign Ownership** dialog box appears.



The image shows a dialog box titled "Assign Ownership". It contains a text input field labeled "Enter the Login ID of User" with the text "super" entered. To the right of the input field is a magnifying glass icon. Below the input field is a checked checkbox labeled "Email Incident to Assigned Owner". At the bottom of the dialog are two buttons: "Submit" and "Cancel".

3. Enter the login ID of the user to whom you want to assign the incident.
If required, click the search icon to display the list of available users.
4. Select the **Email Incident to Assigned Owner** check box to send an e-mail notification to the assigned owners of the incident. This option is selected by default.
5. Click **Submit**.

The incident is assigned to the specified user. See [“Viewing Details of a Device Snapshot” on page 74](#).

Related Documentation

- [Incidents Overview on page 37](#)
- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)

Submitting an Incident to Juniper Support Systems

After viewing the incident information, you can use the Incidents page to submit the incident to Juniper Support Systems (JSS) for creating a case. You can submit multiple incidents to JSS simultaneously. The status of a submitted incident appears in the Status column of the Incidents page. After you submit the incident, the status is displayed as Submitted.



NOTE: The Submitted status is displayed in red if an error or exception has occurred while submitting the incident to JSS. If you place the cursor on Submitted, a tool tip displays the error message.

An error or exception can occur while submitting an incident when there is an issue with Customer Relationship Manager (CRM) in JSS; for example, CRM is down for maintenance. The Submitted status is automatically displayed in black when the CRM becomes functional.

When a case is created by JSS, the status changes to Created and a case ID is generated for the incident.

Before an incident is submitted from Service Now to JSS, the synopsis of the incident is tagged in the Service Now database to indicate whether it is an on-demand or a Return Materials Authorization (RMA) incident generated by AI-Scripts or Service Now. The synopsis of an incident generated by an event on the device is not tagged. An incident is submitted to JSS with one of the following tags:

- *AIS On Demand* for on-demand incidents generated by AI-Scripts
- *On Demand* for on-demand incidents generated by Service Now
- *Express RMA* for RMA incidents detected by AI-Scripts
- *On Demand RMA* for on-demand RMA incidents generated by Service Now

You can submit incidents to JSS as soon as a JMB is received from the device, without downloading attachments from the JMB. Then Service Now automatically uploads the JMB attachments to the related case.

To submit an incident to JSS:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. On the Incidents page, select the incident that you want to submit to JSS.
3. From the Actions menu, select **Submit Case**. Alternatively, right-click the incident and select **Submit Case**.

Figure 7 on page 45 displays the Submit Case Options page cropped up to the Add Comments to the Description field..



NOTE: The Submit Case action is disabled when you select an incident that is already submitted.

Figure 7: Submit Case Options Page

4. Under Email List, click the **Enter Email Id** field to enter an e-mail ID in the user@example.com format.
5. (Optional) To add multiple e-mail IDs or delete them, use the **Add Email** and **Delete** buttons, respectively.
6. (Optional) Click **Modify** to modify the existing site ID or username.

The Make Selection to Change Site ID or User dialog box appears.

The site ID can be modified in two ways:

- For the same username:
 - a. Click **Default Org**.
 - b. Select a site ID from the Site ID list
- For a new user:

- a. In the **Username** field, enter the username to log in to the organization.
The username is provided by Juniper Networks or a Juniper Networks partner.
 - b. In the **Password** field, enter the password to log in to the organization.
The password is provided by Juniper Networks or a Juniper Networks partner.
 - c. Click the **Get Sites** link.
The Site ID list displays a list of site IDs.
 - d. Select the required site ID.
7. (Optional) In the Make Selection to Change Site ID dialog box, select the **Save As Default User For Incident Submission** check box if you want the new site ID to be set as the default site ID. This new site ID and username are displayed by default when you log in next time to submit new incidents.
 8. Click **OK** to save the changes and go back to the Submit Case Options page. Click **Cancel** if you do not want to implement the changes.
 9. (RMA incident only) If you are submitting an RMA incident, on the Submit Case Options page, you must select an **Address Group**.

The **Ship-to Address** field is populated automatically based on the selected address group.

By default, in case of standard, partner proxy, or end customer modes, the Address Group field displays the address group values present in the system. The values displayed in the Address Group and Ship-to Address fields are determined by the following:

- In End Customer and Direct modes, the value displayed in the Address Group and Ship-to Address fields depend on the association between the device and address group. If a user has associated the device with an address group before the incident took place, then the value is preselected in the Address Group field. In case a user associates the device with an address group after the incident took place, then the Location and Ship-to Address fields display None. You can select any other address group present in the system to create a CRM case with JSS or the Juniper Networks partner.
- In Partner Proxy mode, the Address Group and Ship-to Address fields are prepopulated with the address group sent by the customer and the address group present in the system for opening a case. The Juniper Networks partner has the option of changing this value by selecting an address group present in the partner system.
- If the Juniper Networks partner has associated an address with the end-customer device, then that address is displayed in the Address Group and Ship-to Address fields instead of the customer address.
- If no device is associated the address group, the value displayed in the Address Group field is None.

The address group selected on the Submit Case page is submitted as the shipping address to the Juniper Networks partner or JSS.

10. Select the method for follow up on the case from the **Follow Up Method** list. The available options are Email Full Text Update, Email Secure Web Link, and Phone Call.
11. Enter a customer tracking number in the **Customer Tracking Number** field.

The customer tracking number can be any random number that you provide to track your case.



NOTE: Steps 4 through 11 are applicable only when you run Service Now in Partner Proxy or Direct modes.

12. Select the priority of the case from the **Priority** list.

The available options are Critical, High, Medium, and Low. The default priority is Medium.

13. (Optional) Add your comments in the **Add Comments to Synopsis** field.

If you are submitting On-demand or Off-Box incidents to JSS, you can edit the default content in the Synopsis field.

14. (Optional) Add your comments in the **Add Comments to Description** field.

Ensure that your comments contain fewer than 1028 characters.

In partner proxy mode, a table listing core files for the incident is displayed below the Add Comments to Description field.

The columns in the table are described as follows:

- **Core Files**—Complete path to the core file, including the name of the core file
- **Core File Size(in bytes)**—Size of the core file, in bytes

15. Select one or more core files to upload. The core files are uploaded after the case is created for the incident.
16. (Optional) To delete core files from the router after you have uploaded the core files, select the **Delete Core Files from Router after Uploading** check box.
17. (Optional) To view the hardware components in the device, click the **Select Device Components** link next to the Synopsis field.
The Device Physical Inventory Components page appears.
18. Select the device components for which you want to request RMA incidents and click **Submit**.
19. In the **Problem Description** field, enter information about the device components (part number, version, part description, part serial number, and so on).
20. Click **Submit**.

A Job Information dialog box that appears displays the job ID.

Click the job ID to go to the **Job Management** page. You can monitor the status of the job from this page.

21. Navigate back to **Service Central > Incidents**.

The Incidents page appears.

22. On the Incidents page, click the RMA incident that you requested and select **Submit Case** from the Actions menu. Alternatively, right click the RMA incident and select **Submit Case**.

The Submit Case Options page appears.

23. Verify the information on the page and click **Save** to save your settings in the Service Now database and go back to the Incidents page.

24. Click **Submit** to submit the selected incident to JSS.

The Incidents page appears. The Incidents page displays the submission status in the Status column as Submitted.

When a case is created for the incident in JSS, the status of the incident changes to Created and a case ID is generated.

Related Documentation

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Viewing Incident Details on page 40](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)

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 navigation tree, select **Service Central > Incidents**.

The Incidents table appears.

2. Select the incident that you want to flag to a user, and select **Flag to Users** from either the **Actions** list or the right-click menu.

The **Flag to Users** dialog box appears and displays the names of Service Now users.

3. Select the user or users to whom you want to flag the incident.
4. Select the **Email Incident to Flagged Users** check box to send an e-mail notification to all the flagged users.

This option is selected by default.

5. Click **Submit**. The incident is flagged to the selected users.

Related Documentation

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Deleting an Incident on page 56](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)

Viewing a Case in 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.



NOTE: This feature is not available if Service Now is in offline mode.

To view a case in the Case Manager:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.

2. Select the incident whose details you want to view in the Case Manager, and select **View Case in Case Manager** from either the **Actions** list or the right-click menu.

The Juniper Networks Login page appears.



NOTE: If the **View Case in Case Manager** link is not enabled, verify if the case is created.

3. Enter your username 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**.

Related Documentation

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Updating an End-Customer Case on page 52](#)

Exporting a Juniper Message Bundle (JMB) to an HTML file

You can export JMB data along with its attachments as HTML files and save them on your local file system. A JMB is exported as a zipped folder. Logs are not exported. The view of the exported JMB file is the same as of the View JMB page in Service Now. However, the option to download the attachments and log files is not available for an exported JMB file.

You can export JMBs in the following two formats—HTML and Excel.

To export incident data in HTML format:

1. From the Service Now navigation tree, select **Service Central > Incidents**.

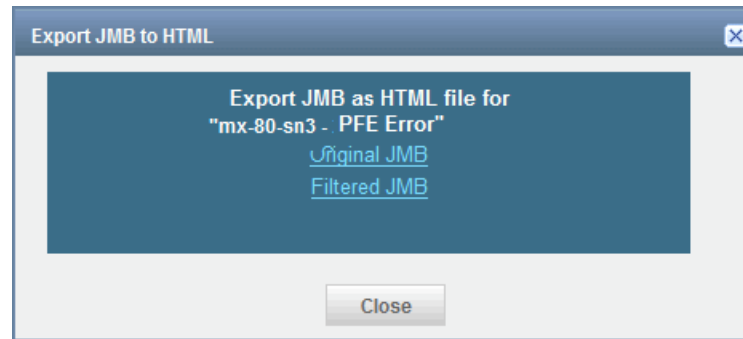
The Incidents page appears.

2. On the Incidents page, select the incident whose details you want to export.

- From the Actions menu, select **Export JMB to HTML**. Alternatively, right-click an incident and select **Export JMB to HTML**.

The Export JMB to HTML dialog box displays links to the original and filtered JMBs, as shown in [Figure 8 on page 51](#).

Figure 8: Export JMB to HTML Dialog Box



- Click the **Original JMB** or **Filtered JMB** link to save the original or filtered JMB file as an HTML file.

To export an incident data as an Excel file:

- From the Service Now navigation tree, select **Service Central > Incidents**.

The Incidents page appears.

- On the Incidents page, select the incident whose details you want to export.
- From the Actions menu, select **Export Incident Summary to Excel**. Alternatively, right-click the incident and select **Export Incident Summary to Excel**.

The **Export Incident Summary to Excel** dialog box displays the Export the selected Incident to Excel link.

- Click the **Export the selected Incident to Excel** link to save the incident data in Excel format.

Related Documentation

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)

Updating an End-Customer Case

In Partner Proxy mode, 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 enabled only when Service Now operates in partner-proxy mode and when the state of the selected case is open.

To update an end-customer case:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page displays the list of incidents.
2. Select the end-customer incident for which you want to create a case, and select **End-Customer Case** from either the **Actions** list or the right-click menu.

The **End-Customer Case** dialog box appears as shown in [Figure 9 on page 52](#).

Figure 9: End-Customer Cases Dialog Box

The dialog box titled "End Customer Cases" contains the following fields and controls:

- Case ID:** ECC1
- Case Link:** [Empty text box]
- Case Status:** Updated (dropdown menu)
- Synopsis:** CHASSISD_FRU_OFFLINE_NOTICE
- Problem Description:**
 - Event message: CHASSISD_FRU_OFFLINE_NOTICE
 - Event description: The chassis process (chassisd) took the indicated component (FPC3) offline for the
- Email List:** user@example.com
- Buttons:** Submit, Cancel

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

3. Modify the case details as necessary.
4. Click **Submit**.

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

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode](#)
- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)

- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)

Uploading an Attachment to an Incident

Service Now provides the Upload Attachment action for an incident to upload a file, for example, a text, image, or binary file, as an attachment to an incident. Only one file can be uploaded at a time. To upload more than one file, compress the files and upload.



NOTE: We recommend that you limit the size of an attachment to be uploaded to 1 GB and use Secure Copy Protocol (SCP) to upload files of size 1 GB.

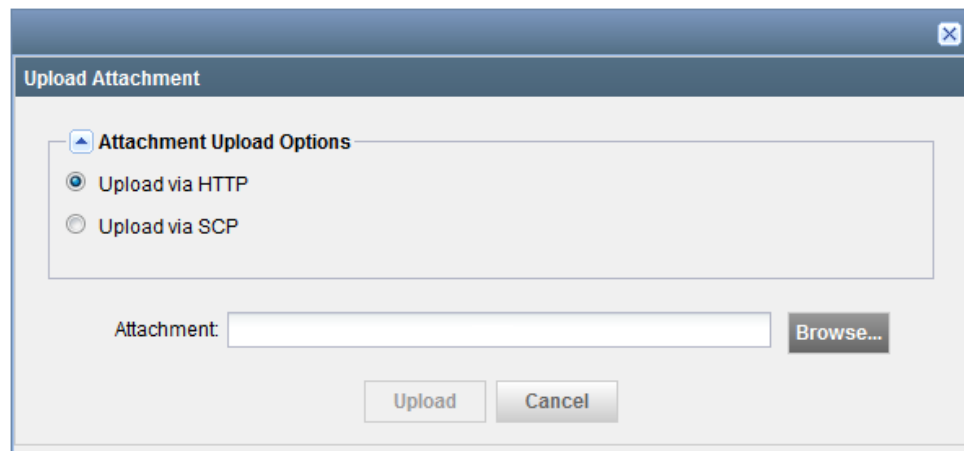
The attachment is stored in Service Now if the incident is not submitted to JSS. If a case is already created for the incident, the attachment, when uploaded to the incident is automatically uploaded to the case as well. The attachment uploaded to Service Now can be viewed on the View JMB page of the incident.

To upload a text or binary attachment to an incident:

1. On the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Select an incident for which you want to upload an attachment.
3. From the Actions menu, select **Upload Attachments**. Alternatively, right-click the incident and select **Upload Attachments**.

The Upload Attachment dialog box appears as shown in figure.

Figure 10: Upload Attachment Dialog Box



4. Under Attachment Upload Options, do one of the following:

- Upload an attachment by using HTTP.

To upload an attachment by using HTTP:

- a. Click **Upload via HTTP**.
- b. Click the **Browse** button to browse for the attachment file and click **Upload**.
The attachment is uploaded to the incident.

- Upload an attachment from a remote machine by using SCP.

To upload an attachment by using SCP:

- a. Click **Upload via SCP**.
- b. Enter the details of the remote machine hosting the attachment as follows:
 - **Username:** Enter the username of the remote machine.
 - **Password:** Enter the password of the local machine.
 - **Confirm Password:** Retype the password.
 - **Machine IP:** Enter the host IP address of the remote machine.
 - **Software File Path:** Specify the path of the attachment file on the remote machine.
- c. Click **Submit**.

The process of uploading the attachment is initiated and the File Upload Job information dialog box appears.

After the upload job is complete, you can view the attachment in the JMB associated with the incident.

- Related Documentation**
- [Technical and End Customer Support Cases Overview on page 59](#)
 - [Incidents Overview on page 37](#)
 - [Uploading an Attachment to a Case on page 64](#)

Uploading Core Files to JSS for an Incident

Using Service Now, you can upload core files generated for an event to Juniper Support Systems (JSS). This function is supported under the following conditions:

- Case should be created for the incident
- At least one core file should be available for upload

If there are no core files available for the incident or if all the core files are uploaded, then this action is disabled in **Incidents**.

To upload core files:

1. From the Service Now navigation tree, select **Service Central > Incidents**.

The **Incidents** page appears.

2. Select the incident whose core files you need to upload, and select **Upload Core Files** from either the **Actions** list or the right-click menu.



NOTE: This action is available only if the incident has any core file to be uploaded. In addition, this action is disabled in the offline and the demo modes.

The **Core File Uploader** dialog box appears with a list of core files.

3. Select the core files that you want to upload, and click **Submit**.
4. If you need to delete the core files from router after uploading, select the **Delete Core Files from Router after Uploading** check box.

- Related Documentation**
- [Incidents Overview on page 37](#)
 - [Submitting an Incident to Juniper Support Systems on page 44](#)
 - [Uploading Core Files Generated for Events](#)
 - [Updating Core File Upload Configuration for an End Customer](#)

Checking Incident Status Updates

In Service Now, incidents are the occurrence of a predefined problem in a device. Information about these incidents is sent to the Service Now application. Service Now routinely checks for new incidents. The **Manage Incidents** page displays the incidents chronologically by organization name and device group.

You can use the Incidents page to submit an incident to JSS for creating a case. The submission status of the incident appears in the Status column on the 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 103](#).
- 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 logged in.

To view the Service Central page, select **Service Central** from the Service Now navigation tree.

Related Documentation

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Deleting an Incident on page 56](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)

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 navigation tree, select **Service Central > Incidents**.

The Incidents table appears.

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
Documentation**

- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 42](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)
- [Updating an End-Customer Case on page 52](#)

CHAPTER 4

Managing Cases

- [Technical and End Customer Support Cases Overview on page 59](#)
- [Updating an End-Customer Case on page 62](#)
- [Uploading an Attachment to a Case on page 64](#)

Technical and End Customer Support Cases Overview

Technical support cases are created in Junos Space Service Now when incidents generated in Service Now are submitted to Juniper Support System (JSS) and a case ID is assigned to the incidents. You can view the technical support cases on the View Tech Support page of the Service Central workspace.



NOTE: Technical support cases cannot be created when Service Now is operating in Demo mode.

When Service Now is operating in End Customer mode, Service Now can submit incidents only to Service Now partner for opening a technical support case. Service Now cannot directly connect with JSS for submitting incidents.

Figure 11 on page 59 shows the View Technical Support Cases page.

Figure 11: View Tech Support Cases

SPACE

User **super** logged in Domain: GlobalSat Jun 20 2015 04:30 AM IST

Applications

Service Now

Dashboard

Service Central

Incidents

View Tech Support Cases

View End Customer Cases

Information

Device Analysis

JMB Errors

Notifications

Devices

Jobs

Administration

Service Central > View Tech Support Cases

Actions -

1 Item Selected

Organization	Site Id	Device Name	Case Id	Device Serial Number	Time Created	Synopsis	Case Type	Priority	Status
TestOrg	99248	2014-0724-0009	CABV4435	Jul 24, 2014 3:24:33 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0803-0002	CABV4435	Aug 3, 2014 7:54:40 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0803-0003	CABV4435	Aug 3, 2014 8:19:23 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0803-0004	CABV4435	Aug 3, 2014 8:19:42 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0803-0005	CABV4435	Aug 3, 2014 8:28:06 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0803-0006	CABV4435	Aug 3, 2014 10:19:48 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0724-0010	CABV4435	Jul 24, 2014 3:24:43 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0803-0008	CABV4435	Aug 4, 2014 6:33:06 AM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0724-0017	CABV4435	Jul 24, 2014 5:14:07 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0801-0317	CABV4435	Aug 1, 2014 4:42:52 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0801-0318	CABV4435	Aug 1, 2014 4:43:00 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0725-0050	CABV4435	Jul 25, 2014 5:18:08 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0727-0010	CABV4435	Jul 28, 2014 10:15:14 AM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0801-0324	CABV4435	Aug 1, 2014 4:46:38 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0801-0323	CABV4435	Aug 1, 2014 4:44:21 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0801-0326	CABV4435	Aug 1, 2014 4:46:57 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0801-0325	CABV4435	Aug 1, 2014 4:46:54 PM IST	Other	2 - High	Open-Initial		
TestOrg	99248	2014-0801-0070	CABV4435	Aug 1, 2014 1:03:29 PM IST	Other	2 - High	Open-Initial		

1 of 108

Displaying 1 - 30 of 108

Table 8 on page 60 lists the columns displayed on the View Tech Support Cases page:

Table 8: Fields on the View Tech Support Cases Page

Field	Description
Organization	Organization to which the device for which the case is created belongs
Site ID	Site ID of organization from which the case was submitted This field is not present if Service Now is operating in the End Customer mode.
Device Name	Name of the device for which the case is created
Case ID	ID of the case
Device Serial Number	Serial number of the device for which the case is created
Time Created	Date and time the case was created in JSS
Synopsis	Synopsis of the incident submitted to create the case
Case Type	Type of the case Possible values are: <ul style="list-style-type: none"> • Event—Case created for events that occurred on devices • Event RMA—Case created for Return Materials Authorization (RMA) events that occurred on devices • On-demand—Case created for on-demand incidents • On-demand RMA—Case created for on-demand RMA incidents • BIOS Health Check—Case created for analyzing BIOS running on devices • AIS Health Check—Case created for AI-Scripts health check events on devices • Event (Low End)—Case created for events that occurred on low-end devices such as SRX100 and SRX220 • Other—Case created for events not reported through Service Now
Priority	Priority assigned to the incident, by the end customer, for which the case is created Possible values are: <ul style="list-style-type: none"> • 1 - Critical • 2- High • 3 - Medium • 4 - Low
Status	Status of the case

A Service Now end customer submits incidents to a Service Now partner. The Service Now partner views the incidents submitted by a Service Now end customer in the Incidents page and, if required, submits them to JSS for creating a technical support case. The Service Now partner can view and track the progress of Service Now end-customer cases

in the View End Customer Cases page of the Service Central workspace. The Service Now partner updates the status of the case to the Service Now end customer.

Figure 12 on page 61 shows the View End Customer Cases page.

Figure 12: View End Customer Cases Page

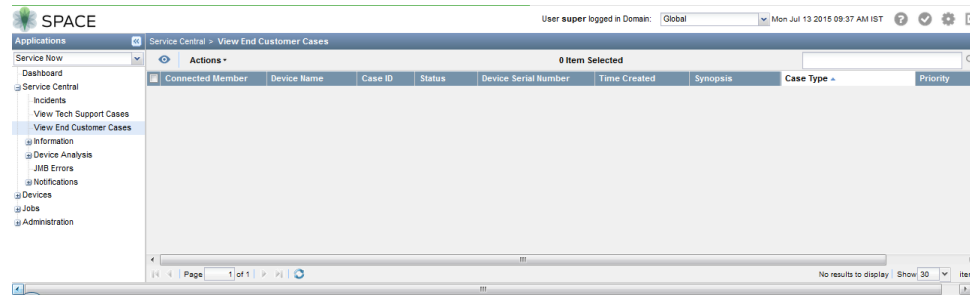


Table 9 on page 61 lists the columns displayed on the View End Customer Cases page:

Table 9: Fields on the View End Customer Cases Page

Field	Description
Connected Member	End customer for whom the case is created
Device Name	Name of the device for which the case is created
Case ID	ID of the case
Status	Status of the case
Device Serial Number	Serial number of the device for which the case is created
Time Created	Date and time the case was created in JSS
Synopsis	Synopsis of the incident submitted to create the case
Case Type	<p>Type of the case</p> <p>Possible values are:</p> <ul style="list-style-type: none"> Event—Case created for events that occurred on devices Event RMA—Case created for Return Materials Authorization (RMA) events that occurred on devices On-demand—Case created for on-demand incidents On-demand RMA—Case created for on-demand RMA incidents BIOS Health Check—Case created for analyzing BIOS running on devices AIS Health Check—Case created for AI-Scripts health check events on devices Event (Low End)—Case created for events that occurred on low-end devices such as SRX100 and SRX220 Other—Case created for events not reported through Service Now

Table 9: Fields on the View End Customer Cases Page (*continued*)

Field	Description
Priority	<p>Priority assigned to the incident, by the end customer, for which the case is created</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2 - High • 3 - Medium • 4 - Low
Related Documentation	<p>You can perform the following tasks from the View Tech Support Cases page:</p> <ul style="list-style-type: none"> • View details of a technical support case in Case Manager; see “Viewing a Case in Case Manager” on page 49 for details. • Add notes to a technical support case; see <i>Adding Notes to a Technical Support Case</i> for details. • Upload binary or text attachments for a technical support case; see “Uploading an Attachment to a Case” on page 64. <p>A Service Now partner can perform the following tasks from the View End Customer Support Cases page:</p> <ul style="list-style-type: none"> • Update an end-customer support case; “Updating an End-Customer Case” on page 52 for details. • View details of an end-customer case in Case Manager; see “Viewing a Case in Case Manager” on page 49 for details.
	<ul style="list-style-type: none"> • Incidents Overview on page 37 • Notification Policies Overview on page 101 • <i>Organizations Overview</i> • <i>Junos Space Service Now Global Settings Overview</i>

Updating an End-Customer Case

In Partner Proxy mode, 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 enabled only when Service Now operates in partner-proxy mode and when the state of the selected case is open.

To update an end-customer case:

1. From the Service Now navigation tree, select **Service Central > Incidents**.
The Incidents page displays the list of incidents.
2. Select the end-customer incident for which you want to create a case, and select **End-Customer Case** from either the **Actions** list or the right-click menu.
The **End-Customer Case** dialog box appears as shown in [Figure 9 on page 52](#).

Figure 13: End-Customer Cases Dialog Box

End Customer Cases

Case ID: ECC1

Case Link:

Case Status:

Synopsis: CHASSISD_FRU_OFFLINE_NOTICE

Problem Description: Event message: CHASSISD_FRU_OFFLINE_NOTICE
Event description: The chassis process (chassisd) took the indicated component (FPC3) offline for the

Email List: user@example.com

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

3. Modify the case details as necessary.
4. Click **Submit**.

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

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Adding an End Customer to Service Now Configured in Partner Proxy Mode](#)
- [Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 42](#)
- [Flagging an Incident to a User on page 48](#)
- [Deleting an Incident on page 56](#)
- [Checking Incident Status Updates on page 55](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 50](#)
- [Submitting an Incident to Juniper Support Systems on page 44](#)
- [Viewing Incident Details on page 40](#)
- [Viewing a Case in Case Manager on page 49](#)

Uploading an Attachment to a Case

Service Now provides the Upload Attachment option to upload a file, for example, a text, image, or binary file, as an attachment to a case created in Juniper Support System (JSS). Only one file can be uploaded at a time. To upload more than one file, compress the files and upload. The attachments you upload are not stored in Service Now; but, details such as name, type of file, size, and time of upload are stored and can be viewed on the



NOTE:

We recommend that you limit the size of an attachment to be uploaded to 1 GB and use Secure Copy Protocol (SCP) to upload files of size 1 GB.

On a Service Now End Customer, attachments uploaded are stored in the Service Now partner.

To upload a text or binary attachment to an incident:

1. On the Service Now navigation tree, select **Service Central > View Tech Support Cases**.

The View Tech Support Cases page appears.

2. Select the technical support case for which you want to upload an attachment.
3. From the Actions menu, select **Upload Attachments**. Alternatively, right-click the technical support case and select **Upload Attachments**.

The Upload Attachment dialog box appears as shown in figure.

Figure 14: Upload Attachment Dialog Box

4. Under Attachment Upload Options, do one of the following:

- Upload an attachment by using HTTP.

To upload an attachment by using HTTP:

- a. Click **Upload via HTTP**.

- b. Click the **Browse** button to browse for the attachment file and click **Upload**.

The attachment is uploaded to the incident.

- Upload an attachment by using Secure Copy Protocol (SCP).

To upload an attachment by using SCP:

- a. Click **Upload via SCP**.
- b. Enter the details of the local machine hosting the attachment as follows:
 - **Username:** Enter your username for the local machine.
 - **Password:** Enter your password for the local machine.
 - **Confirm Password:** Retype your password.
 - **Machine IP:** Enter the host IP address of the local machine.
 - **Software File Path:** Specify the file path to access the Service Now image file on the local machine.
- c. Click **Submit**.

The process of uploading the attachment is initiated and the File Upload Job dialog box displays the progress of the job.

**Related
Documentation**

- [Technical and End Customer Support Cases Overview on page 59](#)
- [Incidents Overview on page 37](#)
- [Uploading an Attachment to an Incident on page 53](#)

CHAPTER 5

Managing Messages

- [Messages Overview on page 67](#)
- [Assigning Ownership to Messages on page 68](#)
- [Flagging a Message to Users on page 68](#)
- [Scanning a Message for Impact on page 69](#)
- [Assigning a Message to an End Customer on page 70](#)
- [Deleting a Message on page 72](#)

Messages Overview

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

You can perform the following tasks in the Information Messages tab:

- Assign an owner to an information message, see [“Assigning Ownership to Messages” on page 68](#) for details.
- Assign messages to connected members.
- Flag an information message to users; see [“Flagging a Message to Users” on page 68](#) for details.
- Delete information messages; see [“Deleting a Message” on page 72](#) for details.
- Scan for devices impacted by the message; see [“Scanning a Message for Impact” on page 69](#) for details.

Related Documentation

- [Device Snapshots Overview on page 73](#)
- [Organizations Overview](#)

Assigning Ownership to Messages

You can assign an owner to every information message for managing any follow up task pertaining to the message.

To assign an owner to an information message:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.

The Messages page appears.

2. Select the information message to which you want to assign an owner, and select **Assign Ownership** from either the **Actions** list or the right-click menu.

The **Assign Ownership** dialog box appears.

3. Enter the login ID of the new owner in the **Enter the Login ID of User** field.
4. Select the **Email Message to Assigned Owner** check box to send an e-mail notification to the assigned owners of the message. This option is selected by default.
5. Click **Submit**.

The specified user is assigned ownership of the selected information message.

Related Documentation

- [Flagging a Message to Users on page 68](#)
- [Scanning a Message for Impact on page 69](#)
- [Deleting a Message on page 72](#)
- [Assigning a Message to an End Customer on page 70](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Messages Overview on page 67](#)
- [Device Snapshots Overview on page 73](#)

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 navigation tree, select **Service Central > Information > Messages**.

The Messages page appears.

2. Select the information message that you want to flag to a user, and select **Flag to Users** from either the **Actions** list or the right-click menu.

The **Flag to Users** dialog box lists the available users.

3. Select one or more users who must be notified of the selected information message.

4. Select the **Email Message to Flagged Users** check box to send an e-mail notification to all the flagged users of the message. This option is selected by default.
5. Click **Submit**.

The specified users are notified of the selected information message and the **Flag** column of that information message displays **Yes**.

**Related
Documentation**

- [Device Snapshots Overview on page 73](#)
- [Assigning Ownership to Messages on page 68](#)
- [Scanning a Message for Impact on page 69](#)
- [Deleting a Message on page 72](#)
- [Assigning a Message to an End Customer on page 70](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Messages Overview on page 67](#)

Scanning a Message for Impact

You can use Service Now to view the devices impacted by the vulnerabilities described in the information message.

To scan iJMBs and view the impacted devices:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.

The Messages page appears.

2. Select the message that you want to scan for impact, and select **Scan for Impact** from either the **Actions** list or the right-click menu.

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 appears:

No impacted devices found.

**Related
Documentation**

- [Device Snapshots Overview on page 73](#)
- [Assigning Ownership to Messages on page 68](#)
- [Flagging a Message to Users on page 68](#)
- [Deleting a Message on page 72](#)
- [Assigning a Message to an End Customer on page 70](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Messages Overview on page 67](#)

Assigning a Message to an End Customer

Service Now polls Juniper Support System (JSS) regularly to receive messages for every configured organization. As a Service Now partner, you can assign multiple messages to a connected member.



NOTE: This action is available only when Service Now operates in partner-proxy mode. For more information about standard, partner-proxy, and end-customer modes, see *Service Now Modes*.

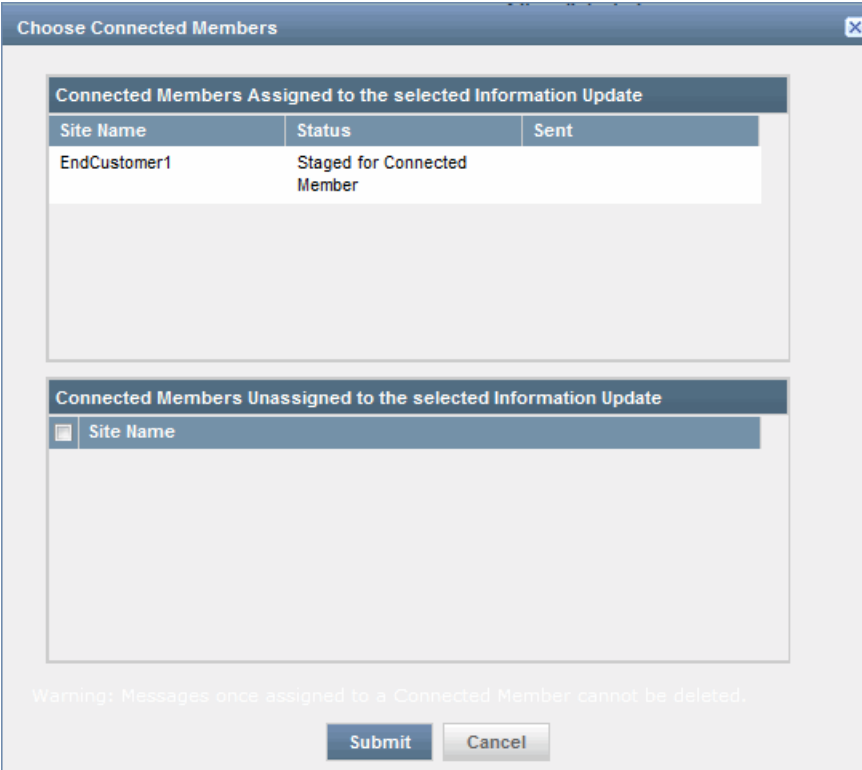
After a message is assigned to a connected member, it cannot be deleted.

To assign a message to a connected member:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.
The Messages page displays the list of information messages received.
2. Select the message that you want to assign to a connected member, and select **Assign Message to End-Customer** from either the **Actions** list or the right-click menu.

As shown in [Figure 15 on page 71](#), the **Choose Connected Members** dialog box displays the list of connected members. It also displays the connected members to whom the message is already assigned along with the status (if any).

Figure 15: Choose Connected Members Dialog Box



The dialog box is titled "Choose Connected Members" and contains two main sections. The first section, "Connected Members Assigned to the selected Information Update", displays a table with the following data:

Site Name	Status	Sent
EndCustomer1	Staged for Connected Member	

The second section, "Connected Members Unassigned to the selected Information Update", contains a search bar with the placeholder text "Site Name". At the bottom of the dialog, there is a warning message: "Warning: Messages once assigned to a Connected Member cannot be deleted." and two buttons: "Submit" and "Cancel".

3. Select the connected member to whom this message must be assigned.
4. Click **Submit**.

The selected message is assigned to the connected member. To verify this action, select **Administration > Organization** to navigate to the Organizations page, and list the messages assigned to any connected member. See *Viewing Messages Assigned to an End Customer*.

Related Documentation

- [Adding an End Customer to Service Now Configured in Partner Proxy Mode](#)
- [Device Snapshots Overview on page 73](#)
- [Assigning Ownership to Messages on page 68](#)
- [Flagging a Message to Users on page 68](#)
- [Scanning a Message for Impact on page 69](#)
- [Deleting a Message on page 72](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Messages Overview on page 67](#)

Deleting a Message

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

To delete an information message:

1. From the Service Now navigation tree, select **Service Central > Information > Messages**.

The Messages page appears.

2. Select the information message that you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.
3. Click **Delete** again to confirm the deletion.

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

Related Documentation

- [Device Snapshots Overview on page 73](#)
- [Assigning Ownership to Messages on page 68](#)
- [Flagging a Message to Users on page 68](#)
- [Scanning a Message for Impact on page 69](#)
- [Assigning a Message to an End Customer on page 70](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Messages Overview on page 67](#)

CHAPTER 6

Managing Device Snapshots or iJMBs

- [Device Snapshots Overview on page 73](#)
- [Viewing Details of a Device Snapshot on page 74](#)
- [Exporting Device Snapshots to HTML on page 76](#)
- [Deleting Device Snapshots on page 77](#)

Device Snapshots Overview

Service Now periodically collects and displays Information Juniper Message Bundles (iJMBs) that contain information about devices. iJMBs are also called device snapshots. They are processed and displayed on the Device Snapshot page in the Service Now application. You can upload these device snapshots to JSS where they are added to the Customer Intelligence Database (CIDB) and then processed and analyzed to provide preventive measures.

You can filter the configuration content from device snapshots that are sent to JSS by setting the JMB Filter Level while creating the organization (See *Adding an Organization to Service Now*) and then track the status of the device snapshot submission to JSS. You can also stop device snapshots from being sent to JSS.

After you install AI-Scripts on a device, device snapshots are sent from each device to Service Now and from Service Now to JSS every 7 days. The configuration information in a device snapshot that is shared with JSS depends on the **JMB Filter Level** settings made while creating the organization to which the devices belongs.

The device snapshots that are received by Service Now and yet to be submitted to JSS are stored with the status **Initial**. After the 7 days elapse, the latest device snapshot sent from the device is submitted to JSS. This means that when a device sends multiple device snapshots to Service Now, only the most recent device snapshot is submitted to JSS and the remaining device snapshots are denoted with the status **Skipped**. Device snapshots are denoted with the Initial status for several reasons. To know why a device snapshot is not submitted to JSS, you can hover over its **Status** in the tabular view of the Device Snapshot page. The **Status** field also displays additional information such as the reasons for not loading information JMBs and messages for errors that might have occurred while loading the JMB.

Devices that have stopped sending iJMBs (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 Quick View of the Device Snapshots page uses different icons to help you identify snapshots that are successfully uploaded to JSS and the device snapshots that could not be uploaded to JSS. For a description of these icons, see *Service Now Icons and Inventory Pages*.

Service Now generates iJMBs automatically for all devices associated to a device group when the devices stop sending iJMBs. The iJMBs are generated based on the commands available in a directive file pre-loaded in Service Now. The behavior of these iJMBs is the same as the iJMBs generated by event scripts. The Service Now administrator receives a message when Service Now generates iJMBs automatically for one or more devices.

Service Now generates iJMBs automatically if:

- Service Now detects that a Junos upgrade has occurred but an event profile is reinstalled, or if Service Now detects that the device has not sent an iJMB for some time
- an event profile was never installed on a device, but the device is associated to a device group in Service Now

If an event profile is installed on the device and an iJMB is received from the device, then Service Now stops creating iJMBs for the device. If the notification policy **Switch over enabled for iJMB** is enabled, the administrator is notified by an e-mail or an SNMP Trap when Service Now generates iJMBs for one or more devices. If the notification policy **Switch over enabled for iJMB** is not enabled, only e-mails are sent to the administrator when Service Now generates iJMBs. No SNMP traps are sent.

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

- Export device data in HTML format; see [“Exporting Device Snapshots to HTML” on page 76](#) for details.
- Delete a device snapshot; see [“Deleting Device Snapshots” on page 77](#) for details.
- View device snapshot details; see [“Viewing Details of a Device Snapshot” on page 74](#) for details.

Related Documentation

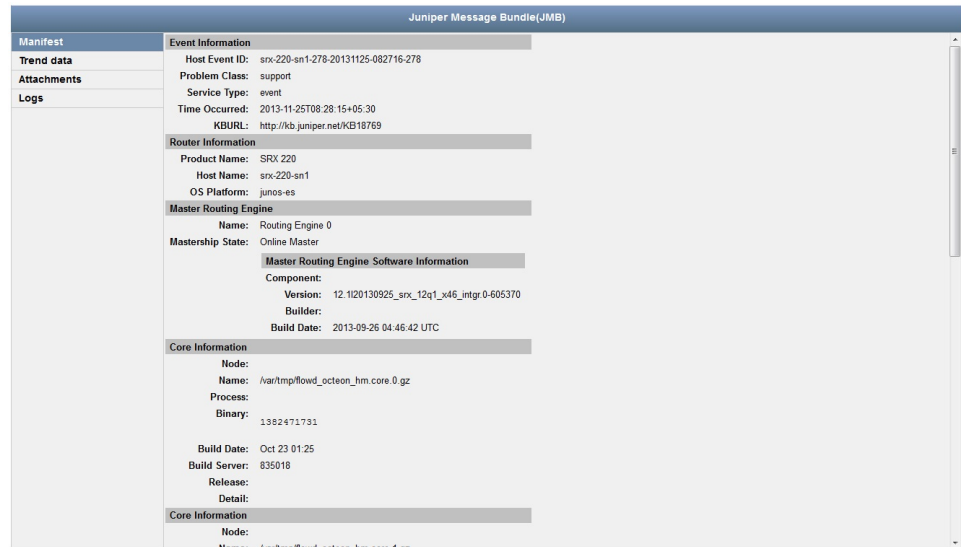
- [Messages Overview on page 67](#)
- [Monitoring Device Snapshots](#)
- [Adding an Organization to Service Now](#)
- [AI-Scripts Overview](#)

Viewing Details of a Device Snapshot

When Service Now receives informational JMBs or iJMBs, only selected information from the JMBs appears on the Device Snapshots page. However, you can view the entire contents of the JMB on the View JMB page.

Service Now displays the JMBs generated by AI-Scripts Release 3.7 and earlier on a single page. For JMBs generated by AI-Scripts Release 4.0 and later, the View JMB page has a right and a left pane. The left pane lists the sections of a JMB. Clicking a section displays the contents of the section in the right pane. When the View JMB page opens, by default, the Manifest section opens as shown in [Figure 16 on page 75](#). You can click the links in the Attachments and Logs sections to view or download attachments and system log files.

Figure 16: Juniper Message Bundle

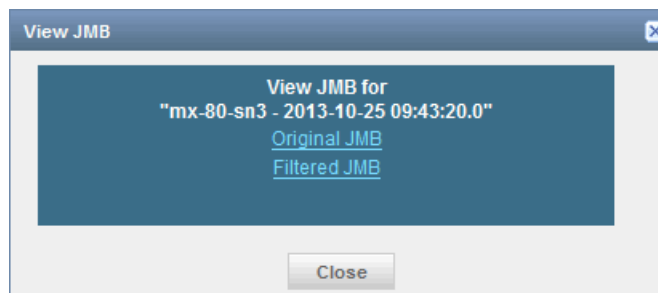


To view details of a JMB:

1. From the Service Now navigation tree, select **Service Central > Information > Device Snapshots**.
The Device Snapshots page appears.
2. On the Device Snapshots page, select the device for which you want to view an iJMB.
3. From the Actions menu, select **View JMB**. Alternatively, right-click the device and select **View JMB**.

The **View JMB** dialog box displays links to the original and the filtered JMBs as shown in [Figure 17 on page 76](#). The information in the filtered JMB is classified by the settings on your Global Settings page.

Figure 17: View JMB Dialog Box



4. Click the **Original JMB** or **Filtered JMB** link to view the JMB details.

Clicking **Original JMB** displays the JMB as received from the device. Clicking **Filtered JMB** displays the JMB after filtering data as configured in the filter criteria.

Related Documentation

- [Device Snapshots Overview on page 73](#)
- [Exporting Device Snapshots to HTML on page 76](#)
- [Deleting Device Snapshots on page 77](#)
- [Messages Overview on page 67](#)

Exporting Device Snapshots to HTML

You can store the device data that Service Now collects and displays on the Device Snapshots page and export it to HTML format.

To export device data to HTML format:

1. From the Service Now navigation tree, select **Service Central > Information > Device Snapshots**.

The Device Snapshots page displays the device snapshots received.

2. Select the organization whose data you want to export, and select **Export to HTML** from either the **Actions** list or the right-click menu.

The **Export JMB to HTML** dialog box displays links to the original and filtered versions of the JMB.

3. Click the displayed link to save the iJMB as an HTML file.

Related Documentation

- [Device Snapshots Overview on page 73](#)
- [Deleting Device Snapshots on page 77](#)
- [Viewing Details of a Device Snapshot on page 74](#)
- [Messages Overview on page 67](#)

Deleting Device Snapshots

Service Now collects and displays device snapshots or iJMBs collected from devices on the Device Snapshots page. Device snapshots are by default stored for 180 days in the Service Now database. The number of days the device snapshots can be stored is configured on the Device Snapshot Purge Time (in days) parameter on the Global Settings page.

Service Now provides the Delete option on the Actions menu for a device snapshot to delete it when required.

To delete a device snapshot:

1. From the Service Now navigation tree, select **Service Central** > **Information** > **Device Snapshots**.

The Device Snapshots page appears.

2. Select the organization whose device information you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.
3. Click **Delete** again to confirm the deletion.

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

Related Documentation

- [Device Snapshots Overview on page 73](#)
- [Exporting Device Snapshots to HTML on page 76](#)
- [Viewing Details of a Device Snapshot on page 74](#)
- [Messages Overview on page 67](#)
- *Junos Space Service Now Global Settings Overview*

CHAPTER 7

Managing BIOS Validations

- [BIOS Validation Overview on page 79](#)
- [Exporting BIOS Validation Results on page 82](#)
- [Deleting BIOS Validation Results on page 84](#)

BIOS Validation Overview

Using Junos Space Service Now, you can analyze the BIOS image installed on a device running Junos OS and verify the integrity of the BIOS image. When you enable and configure BIOS validation on a device, AI-Scripts installed on the device collect the BIOS image data from the device. In response to the BIOS image data collected, BIOS validation incidents are created in Service Now and the collected BIOS data is submitted to Juniper Support System (JSS) to create a BIOS Health Check case. In response to the BIOS Health Check case, JSS validates the BIOS image data from the device and sends the validation result to Service Now.

A Service Now partner can accept or reject data for BIOS validation sent by a Service Now end customer. If a Service Now partner chooses to accept the data for BIOS validation from a Service Now end customer, the Service Now end customer submits the BIOS data to the Service Now partner which in turn submits the BIOS data to JSS for validation. If the Service Now partner chooses not to accept BIOS validation data from a Service Now end customer, the option to configure BIOS data validation is disabled on the Service Now end customer. For information about disabling BIOS validation on a Service Now end customer, see *Adding an End Customer to Service Now Configured in Partner Proxy Mode*.

Before you configure BIOS validation, you must accept the BIOS legal notice. The BIOS legal notice is presented to you when you configure BIOS validation for the first time on a Service Now device on a fresh Service Now installation. The BIOS legal notice is also presented when you remove all devices from Service Now and configure BIOS validation after adding the device back to Service Now.

[Figure 18 on page 80](#) and [Figure 19 on page 80](#) show the legal notice displayed on Service Now operating in Partner Proxy and End Customer modes.

Figure 18: BIOS Validation Legal Notice on Service Now Partner

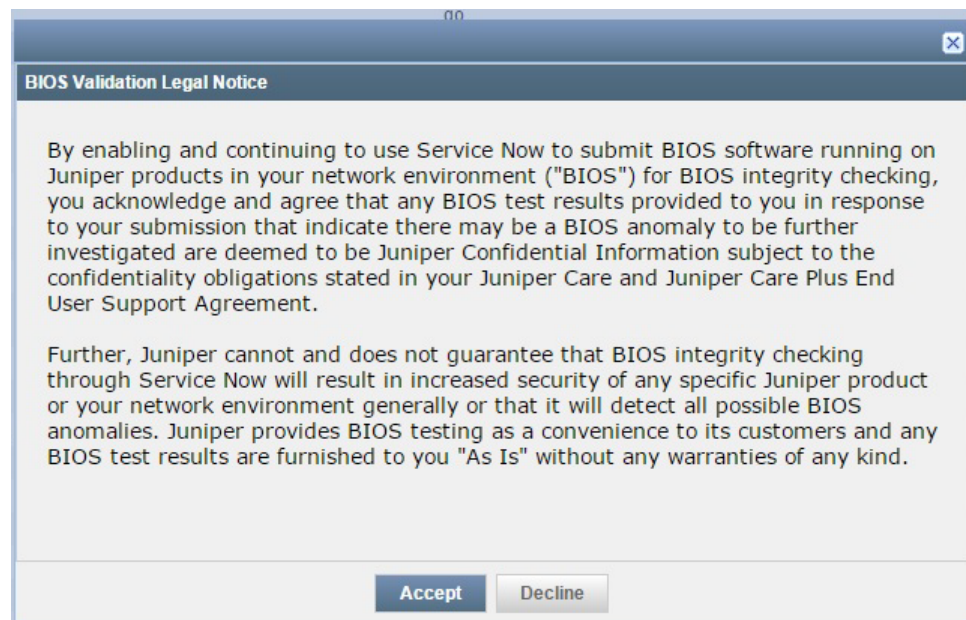
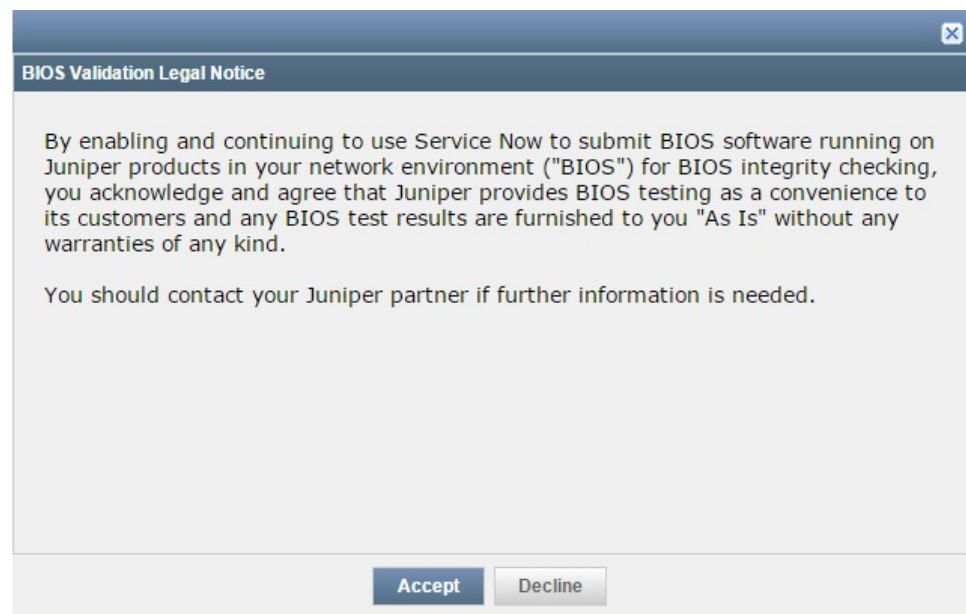


Figure 19: BIOS Validation Legal Notice on Service Now End Customer



On its dashboard, the Device Analysis task displays the status and results of the BIOS validations for all managed devices. Service Now compares the BIOS images received from different devices in a day and submits only the unique BIOS images to JSS for creating BIOS Validation cases; that is, if the same BIOS image is received from thousand managed devices in a day, thousand different incidents are created on Service Now, but only the unique BIOS image is submitted to JSS and one case is created for BIOS validation. If two unique BIOS images are received from managed devices in a day, the two unique images are submitted to JSS and two cases for BIOS validation are created.

A maximum of hundred BIOS Health Check cases can be submitted to JSS from an organization in any given day.

To view the status of BIOS validation, on the Service Now navigation tree, select **Service Central > Device Analysis > BIOS Validations**. The BIOS Validations page appears.

[Table 10 on page 81](#) lists the information displayed by the BIOS validations report.

Table 10: BIOS Validations Field Descriptions

Field Name	Description
Incident Details	
Organization	Organization to which the device for which BIOS validation was performed belongs
Device Group	Device group to which the device for which BIOS validation was performed belongs
Connected Member	End customer to which the device belongs if Service Now is operating in Partner Proxy mode
Device	Device for which BIOS validation was performed
Product	Product family to which the device belongs
Entity	Routing Engine of the device for which BIOS validation was performed
Junos Version	Version of Junos OS installed on the device
Occurred	Date and time when data about BIOS running on the device was collected.
Status	<p>Status of BIOS validation:</p> <ul style="list-style-type: none"> Pending Submission—Service Now has received data for BIOS validation from the device; the data is yet to be submitted to Juniper Support System (JSS). Pending Case Creation—BIOS validation data of the device is received by JSS; JSS is yet to create a case for the received data. Case Created—JSS has created a case for the BIOS validation data received for the device. NOTE: This status is not applicable when Service Now is operating in End Customer mode. Case Creation Failed—JSS failed to create a case for the BIOS validation data received for the device. NOTE: This status is not applicable when Service Now is operating in End Customer mode. Submission Failed—Service Now is unable to submit the BIOS validation data of the device to JSS. Validation Success—Validation of BIOS data by JSS was successful. Out for Extended Review—The BIOS validation encountered issues and the BIOS data is sent to the device team for further review.
Attachment Details	

Table 10: BIOS Validations Field Descriptions (*continued*)

Field Name	Description
Attachment	Name of the attachment file You cannot view the contents of the attachment file.
Attachment Size (in byte)	Size of the attachment file in bytes
Command	Command issued on the device to obtain the attachment file
Read Status	Status of reading the attachment from the device
Remarks	Remarks about the attachment.
Log File Details	
Log File	The system log file collected as part of BIOS validation You cannot view the contents of the system log files.
Log File Size (in bytes)	Size of log files in bytes.
Read Status	Status of reading the log files
Remarks	Remarks about the log files.

From the BIOS Validations page, you can perform the following:

- Delete BIOS validations; see [“Deleting BIOS Validation Results” on page 84](#)
- Export information about BIOS validation results to Excel, see [“Exporting BIOS Validation Results” on page 82](#)

Related Documentation

- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device](#)
- [Product Health Data Collection Overview on page 85](#)

Exporting BIOS Validation Results

You can export the results of BIOS validations of managed devices to an Excel file for reference. [Table 11 on page 82](#) lists the BIOS validation information exported to an Excel file.

Table 11: BIOS Validation Field Descriptions

Field Name	Description
Organization	Organization to which the device for which BIOS validation was performed belongs
Device Group	Device group to which the device for which BIOS validation was performed belongs

Table 11: BIOS Validation Field Descriptions (*continued*)

Field Name	Description
Connected Member	End customer to which the device belongs; this field is applicable only for a Service Now partner.
Hostname	Hostname of the device from which BIOS data was collected
IP address	IP address of the device from which BIOS data was collected
Entity	Routing Engine of the device for which BIOS validation was performed
BIOS Result	Status of BIOS validation: <ul style="list-style-type: none"> • Pending Submission—Service Now has received data for BIOS validation from the device; the data is yet to be submitted to Juniper Support System (JSS). • Submitted—Service Now has submitted the BIOS data to JSS for validation. • Submission Failed—Service Now is unable to submit the BIOS validation data of the device to JSS. • Validation Success—Validation of BIOS data by JSS was successful. • Out for Extended Review—The BIOS validation encountered issues and the BIOS data is sent to the device team for further review.
Time Received	Time when the last update of BIOS validation was received from JSS
Junos Version	Version of Junos OS running on the Routing Engine of the device
AI-Scripts Version	Version of AI-Scripts installed on the device

To export BIOS validation results:

1. From the Service Now navigation tree, select **Service Central > Device Analysis > BIOS Validations**.

The BIOS Validations page appears.

2. Select one or more BIOS validation results to be exported.
3. From the Actions menu, select **Export to Excel**. Alternatively, right-click the device and select **Export to Excel**.

The Export BIOS Validations to Excel dialog box appears.

4. Click the **Export the selected BIOS Validations to Excel** link.

The dialog box of the browser to open or save the Excel file appears.

5. Click **Open with** to open the file or click **Save File** to save the file.

Related Documentation

- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device](#)
- [BIOS Validation Overview on page 79](#)
- [Deleting BIOS Validation Results on page 84](#)

Deleting BIOS Validation Results

You can delete results of BIOS validations when you no longer need them. Junos Space Service Now does not let you delete a BIOS validation result if the status is Pending Case Creation or Case Created. However, on a Service Now end customer, BIOS validations can be deleted irrespective of its status.

To delete BIOS validation results:

1. From the Service Now navigation tree, select **Service Central > Device Analysis > BIOS Validations**.

The BIOS Validations page appears.

2. Select one or more BIOS validation results to be deleted.
3. From the Actions menu, select **Delete BIOS Validations**. Alternatively, right-click the device and select **Delete BIOS Validations**.

The Delete BIOS Validations dialog box appears.

4. Click **Delete** to delete the BIOS validation results or **Cancel** to cancel the deletion.

If you click Delete, the BIOS validation results you selected are no longer listed on the BIOS Validations page.

Related Documentation

- [BIOS Validation Overview on page 79](#)
- *Configuring BIOS Validation for Verifying BIOS Integrity of a Device*
- [Exporting BIOS Validation Results on page 82](#)

CHAPTER 8

Analyzing Physical Health Data

- [Product Health Data Collection Overview on page 85](#)
- [Exporting Product Health Data Information to an Excel File on page 87](#)
- [Viewing Product Health Data Files Collected from a Device on page 92](#)
- [Deleting Product Health Data Files Collected from a Device on page 95](#)

Product Health Data Collection Overview

You use the product health data collection (PHDC) feature of Junos Space Service Now to collect product health data (PHD) from managed devices. PHD is used to assess the health of the devices.



NOTE:

- PHDC is not supported on Service Now operating in End Customer mode.
- PHDC is not supported on QFX Series devices in a QFabric.
- PHD can be collected only if AI-Scripts 5.0 or later is installed on a device.
- Within the Service Now application, the product health data collection term, in addition to indicating the feature, indicates individual product health data collection configuration.

PHD comprise the output of various **show** commands of Junos OS, such as **show version**, **show system uptime**, **show chassis fabric summary**, and so on. AI-Scripts installed on managed devices execute the **show** commands and collect the output as a Juniper Message Bundle (JMB). AI-Scripts execute the **show** commands at one-hour interval for the configured number of days. Service Now collects the JMBs and creates a PHD file. The PHD file can be viewed from **Service Central > Device Analysis > Product Health Data Devices** and **Administration > Product Health Data Collection** tasks of the Service Now navigation tree. For information about viewing PHD files, see [“Viewing Product Health Data Files Collected from a Device” on page 92](#).

[Figure 20 on page 86](#) shows the Product Health Data Devices page that lists the devices from which PHD are collected. You can view the status of PHDC on a device on this page. A device is listed on this page when at least one PHD file is collected from it.

Figure 20: Product Health Data Devices Page

Device	Serial Number	Product	View
snx-220-sn1	AQ5210AA0078	SRX220H	View
snx-650-sn2	AJ4410AA0037	SRX650	View

Table 12 on page 86 describes the fields on the Product Health Data Devices page.

Table 12: Fields on the Product Health Data Devices Page

Field Name	Description
Device	Name of the managed device from which PHD is collected
Serial Number	Serial number of the device
Product	Type of Junos product
View	<p>Link to view the PHD files collected from the device</p> <p>For information about viewing the PHD files, see “Viewing Product Health Data Files Collected from a Device” on page 92.</p>

The collected PHD is submitted to Juniper Support System (JSS) that assesses the health of the device. JSS submits the result of the assessment to the Juniper Networks customer who requested the PHD assessment.

To configure PHDC on Service Now, define the following:

- Devices from which PHD should be collected
- Number of days for which PHD should be collected from the devices
- Whether PHD should be uploaded to JSS
- Whether PHD should be deleted from Service Now after it is uploaded to JSS
- Whether IP addresses should be overwritten with asterisks (*) for security purposes in the PHD files

You can configure PHDC on a device in one of the following ways:

- From the Product Health Data Collection task of the Administration workspace
- From the Service Now Devices task of the Administration workspace

For information about configuring PHDC on managed devices, see *Configuring Product Health Data Collection on a Device*.

From the Product Health Data page, you can perform the following tasks:

- Export information about devices from which PHD is collected to Excel.
- Export information about the collected PHD files of a device to Excel.

For information about exporting PHD to Excel, see “[Exporting Product Health Data Information to an Excel File](#)” on page 87.

Related Documentation

- *Product Health Data Collection Configuration Overview*
- [BIOS Validation Overview](#) on page 79

Exporting Product Health Data Information to an Excel File

Junos Space Service Now provides the Export and Export All options on the Product Health Data Devices task to export the following information in an Excel file:

- Devices on which product health data collection (PHDC) is configured

The exported Excel file is named in the format **PHDDevices_yyyy-mm-dd_hhmmss**, where *yyyy-mm-dd* and *hhmmss* are the date and time the Excel file is created.

[Figure 21 on page 87](#) shows a sample of the information about devices exported to Excel.

Figure 21: PHDC Information of Devices Exported to Excel

	A	B	C	D	E	F	G	H
1								
2	Device	Serial Number	PHD Group Name	Start Date	Status	Total Files Received	Last Uploaded	Status Message
3	mx-80-sn2	D4358	Test-group	2015-07-16 01:32:51.36	Running	28		
4	mx-480-sn1	JN11AFF42AFB	Test-group	2015-07-16 01:32:51.36	Running	28		
5								
6								

- Product health data (PHD) files collected from individual devices

The exported Excel file is named in the format

PHDInfoReport-hostname_yyy-mm-dd_hhmmss, where *hostname* is the hostname of the device from which the PHD files were collected and *yyyy-mm-dd* and *hhmmss* are the date and time the Excel file is created.

[Figure 22 on page 88](#) shows a sample of the information about PHD files exported to Excel.

Figure 22: PHD Files Information Exported to Excel

	A	B	C	D	E	F	G
1							
2	Device Name	mx-480-sn1					
3	Total Number of PHD	25					
4							
5	File Name	Group Name	Size (Bytes)	Received (UTC)	Read Status	Upload Status	Remarks
6							
7	mx-480-sn1_phdc_jmb	Test-group	59548	2015-07-16 10:18:08.15	Success	Success	
8	mx-480-sn1_phdc_jmb	Test-group	59984	2015-07-16 23:18:06.51	Success	Not Uploaded	
9	mx-480-sn1_phdc_jmb	Test-group	N/A	2015-07-17 02:19:22.55	Not Received	Not Uploaded	
10	mx-480-sn1_phdc_jmb	Test-group	59561	2015-07-16 13:18:03.25	Success	Success	
11	mx-480-sn1_phdc_jmb	Test-group	90203	2015-07-16 02:19:16.46	Success	Success	
12	mx-480-sn1_phdc_jmb	Test-group	59552	2015-07-16 05:18:07.90	Success	Success	
13	mx-480-sn1_phdc_jmb	Test-group	59758	2015-07-16 16:18:03.51	Success	Success	
14	mx-480-sn1_phdc_jmb	Test-group	59561	2015-07-16 19:18:08.45	Success	Not Uploaded	
15	mx-480-sn1_phdc_jmb	Test-group	59416	2015-07-16 06:18:01.12	Success	Success	
16	mx-480-sn1_phdc_jmb	Test-group	59832	2015-07-16 22:18:06.82	Success	Not Uploaded	
17	mx-480-sn1_phdc_jmb	Test-group	59812	2015-07-16 09:18:03.65	Success	Success	
18	mx-480-sn1_phdc_jmb	Test-group	59569	2015-07-17 01:18:07.51	Success	Not Uploaded	
19	mx-480-sn1_phdc_jmb	Test-group	59556	2015-07-16 12:18:03.25	Success	Success	
20	mx-480-sn1_phdc_jmb	Test-group	59563	2015-07-16 15:18:10.06	Success	Success	
21	mx-480-sn1_phdc_jmb	Test-group	59949	2015-07-16 03:18:01.24	Success	Success	

To export PHDC data in Excel format, see the following:

- [Exporting Information about Devices on which PHDC is configured on page 88](#)
- [Exporting Data about PHD Files Collected from a Device on page 90](#)

Exporting Information about Devices on which PHDC is configured

You can export Information about devices on which PHDC is configured from the Product Health Data Devices task or the Product Health Data Collection task of the Service Now navigation tree. When you export information about devices from the Product Health Data Devices task in Service Central workspace, information about all the managed devices in Service Now from which PHD is collected is exported; whereas, when you export information about devices from the Product Health Data Collection task in the Administration workspace, information about devices in a specific PHDC configuration is exported.

To export information about devices on which PHDC is configured to Excel:

1. • To export the information from the Product Health Data Devices task:
 - a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- To export the PHD files from the Product Health Data Collection task:
 - a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- b. Click the link on the Devices column of a PHDC configuration.

The View all Devices of this PHDC page appears as shown in [Figure 23 on page 89](#). The View all Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 23: View all Devices of this PHDC

Device	Serial Number	Product	Start Date	Status	Total Files Available
snx-220-sn1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
snx-650-sn2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 AM IST	Running	0

2. • To export information about all the devices, right-click on a row and select **Export All**.

The Export All Product Health Data Devices dialog box is displayed. The dialog box displays the **Export All Product Health Data Devices to Excel** link to download the Excel file.

- To export information about selected devices, select the devices and then right-click and select **Export Selected**.

The Export Selected Product Health Data Devices dialog box is displayed. The dialog box displays the **Export selected Product Health Data Devices to Excel** link to download the Excel file.

3. Click the **Export selected Product Health Data Devices to Excel** or **Export All Product Health Data Devices to Excel** link displayed on the dialog box.

The dialog box of your browser to open or save a file appears.

4. Choose the option to open or save the Excel file.

Exporting Data about PHD Files Collected from a Device

You can export the PHD files from the Product Health Data Devices task in the Service Central workspace or the Product Health Data Collection task in the Administration workspace of the Service Now navigation tree.

To export data about PHD files collected from a device:

1. • To export the PHD files from the Product Health Data Devices task:
 - a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- b. Click the **View** link of the device for which you want to export PHD files.

The View All Product Health Data Files page appears as shown in [Figure 24 on page 91](#).

Figure 24: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_182001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

- To export the PHD files from the Product Health Data Collection task:
 - a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- b. Click the link in the Devices column of a PHDC configuration.

The View All Devices of this PHDC page appears as shown in [Figure 25 on page 91](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 25: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
sr1-220-sr1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
sr1-650-sr2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 AM IST	Running	0

- c. Click the link in the Total Files Available column for the device for which you want to export the PHD files.

The View all Product Health Data Files page appears.

2. • To export information about all the PHD files collected for the device, right-click a row on the page and select **Export All**.

The Export All Product Health Data Information dialog box is displayed. The dialog box contains the **Export all Product Health Data files information to Excel** link to download the Excel file.

- To export information about selected PHD files, select the files to be exported and then right-click and select **Export**.

The Export Selected Product Health Data Information dialog box is displayed. The dialog box contains the **Export selected Product Health Data files information to Excel** link to download the Excel file.

3. Click the **Export selected Product Health Data files information to Excel** or **Export all Product Health Data files information to Excel** link displayed on the dialog box.

The dialog box of your browser to open or save a file appears.

4. Choose the option to open or save the Excel file.

Related Documentation

- [Product Health Data Collection Overview on page 85](#)
- [Viewing Product Health Data Files Collected from a Device on page 92](#)
- [Product Health Data Collection Configuration Overview](#)

Viewing Product Health Data Files Collected from a Device

Junos Space Service Now stores product health data (PHD) as PHD files in the Service Now database. From the database, these files are uploaded to Juniper Support System (JSS) for assessment. To view the list of PHD files in the Service Now database, use the View all PHD for this device page, shown in [Figure 26 on page 92](#). You also use this page to download, export, and delete the PHD files.

You can access the View All Product Health Data Files page from the Product Health Data Devices task or the Product Health Data Collection task of the Service Now navigation tree.

Figure 26: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sr1_phdc_jmb_ais_health_20150416_162001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sr1_phdc_jmb_ais_health_20150416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

Table 13: Fields on the View All Product Health Data Files Page

Field Name	Description
File Name	<p>Name of the PHD file</p> <p>The name is specified in the following format: <code>hostname-sys_phdc_jmb_ais_health_yyyymmdd_hhmmss</code>, where</p> <ul style="list-style-type: none"> • <code>hostname</code> is the hostname of the device from which PHD is collected. • <code>yyymmdd</code> is the date when PHD was collected. • <code>hhmmss</code> is the time when PHD was collected.
PHDC Name	PHDC configuration used to collect PHD
Received	Date and time when Service Now collected PHD
File Size (Bytes)	Size of the PHD file in bytes
Read Status	<p>Read status of PHD from the device</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Not Received—Service Now has not yet collected PHD from the device. • Success—Service Now has successfully collected PHD from the device. • Failure—Service Now failed to collect PHD from the device. • No Longer Available— PHD is no longer available on the device. • Successfully Deleted—PHD is successfully deleted from the device after collection by Service Now. • Reading from Device—Service Now is currently reading PHD from the device. • Read Complete—Service Now has completed reading PHD from the device. • Processing—Service Now is processing PHD to create the PHD files.
Upload Status	<p>Status of uploading PHD files to JSS:</p> <ul style="list-style-type: none"> • Not Uploaded—Service Now has not yet uploaded PHD files to JSS. • Success—Service Now has successfully uploaded PHD files to JSS. • Failure—Upload of PHD files to JSS failed. • Uploading—Service Now is uploading PHD files to JSS.
Remarks	Remarks about a failed condition such as failure to read PHD from the device or upload a PHD file to JSS

To view the PHD files collected from a device:

1. • To access the View All Product Health Data Files page from the Product Health Data Devices task:

- a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- b. Click the **View** link of the device for which you want to view PHD files.

The View All Product Health Data Files page appears.

- To access the View All Product Health Data Files page from the Product Health Data Collection task:

- a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- b. Click the link in the Devices field of a PHDC configuration.

The View All Devices of this PHDC page appears as shown in [Figure 27 on page 94](#).

The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 27: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
sn-220-sn1	AG5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
sn-650-sn2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 AM IST	Running	0

- c. Click the link in the Total Files Available field for the device for which you want to view the PHD files.

The View All Product Health Data Files page appears.

2. On the View All Product Health Data Files page, click one or more files that you want to select for download.
3. Right-click the selection and select **Download Product Health Data File**.

The Download Product Health Data Files dialog box appears.

4. Click the **Download** button.

The Product Health Data Files Download Job Status dialog box appears. The dialog box displays the Download link after the download job is complete.

5. Click the **Download** link.

The dialog box of your browser to open or save the file appears.

6. Click the option to open or save the downloaded file.

The product health data file is downloaded as a ***.zip** file.

7. Extract the PHD file and view the contents on any text editor such as Notepad or Wordpad.

Related Documentation

- [Product Health Data Collection Overview on page 85](#)
- [Product Health Data Collection Configuration Overview](#)
- [Exporting Product Health Data Information to an Excel File on page 87](#)
- [Deleting Product Health Data Files Collected from a Device on page 95](#)
- [Deleting a Product Health Data Collection Configuration from Service Now](#)

Deleting Product Health Data Files Collected from a Device

The product health data (PHD) files collected from managed devices are stored in Junos Space Service Now database and uploaded to Juniper Support System (JSS) for assessing the health of the device. If configured to be deleted, the PHD files are deleted immediately after they are uploaded to JSS. Otherwise, the PHD files are deleted from the Service Now database four days after they are created.

Service Now provides the delete option to delete the PHD files if you want to delete the PHD files. You can delete the PHD files from the Product Health Data Devices task in the Service Central workspace or the Product Health Data Collection task in the Administration workspace of the Service Now navigation tree.

To delete the PHD files collected from a device:

1. • To delete the PHD files from the Product Health Data Devices task of the Service Central workspace:
 - a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

The Product Health Data Devices page appears.

- b. Click the **View** link of the device for which you want to delete PHD files.

The View All Product Health Data Files page appears as shown in [Figure 28 on page 96](#).

Figure 28: View All Product Health Data Files Page

Service Central > Device Analysis > Product Health Data Devices > View all Product Health Data Files						
File Name	PHDC Name	Received ~	File Size (Bytes)	Read Status	Upload Status	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_182001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21450	Success	Uploaded	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded	
ex-4200-sr1_phdc_jmb_ais_health_2015_0416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded	

- To delete the PHD files from the Product Health Data Collection task of the Administration workspace:
 - From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

The Product Health Data Collection page appears.

- Click the link in the Devices field of a PHDC configuration.

The View All Devices of this PHDC page appears as shown in [Figure 29 on page 96](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 29: View All Devices of this PHDC Page

Administration > Product Health Data Collection > View all Devices of this PHDC						
Device	Serial Number	Product	Start Date	Status	Total Files Available	
snx-220-sn1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:15:00 AM IST	Running	0	
snx-650-sn2	AJ4410AA0037	SRX650	Aug 27, 2015 10:15:00 AM IST	Running	0	

- Click the link in the Total Files Available field for the device for which you want to delete the PHD files.

The View All Product Health Data Files page appears.

2. On the View All Product Health Data Files:

- To delete selected PHD files, select the files that you want to delete and then select **Delete Product Health Data**.

The Delete Selected Product Health Data Files dialog box appears.

- To delete all the PHD files collected from the device, right-click any row and select **Delete All Product Health Data**.

The Delete All Product Health Data Files dialog box appears.

3. Click the **Delete** button to delete or the **Cancel** button to cancel the deletion.

If you click the Delete button, a message indicating that the files are deleted is displayed.

**Related
Documentation**

- [Product Health Data Collection Overview on page 85](#)
- *Product Health Data Collection Configuration Overview*
- [Viewing Product Health Data Files Collected from a Device on page 92](#)
- [Exporting Product Health Data Information to an Excel File on page 87](#)

CHAPTER 9

Managing JMB with Errors

- [JMBs with Errors on page 99](#)

JMBs with Errors

Service Now considers a Juniper Message Bundle (JMB) as erroneous if it does not comply with the standard data structure that Service Now accepts or if the Manifest section of the JMB is incorrect. From AI-Scripts Release 4.0, an incomplete Trend Data section or an incomplete attachment in the Attachment section in the JMB is ignored.

Service Now identifies the JMBs with errors and displays them on the JMB Errors page. You can download up to five JMB files at a time and also delete them from the Service Now database. We recommend that you open a case with JSS for JMBs with errors.

Refer to the following topics to download or delete JMBs with errors:

- [Downloading JMBs with Errors on page 99](#)
- [Deleting JMBs with Errors on page 100](#)

Downloading JMBs with Errors

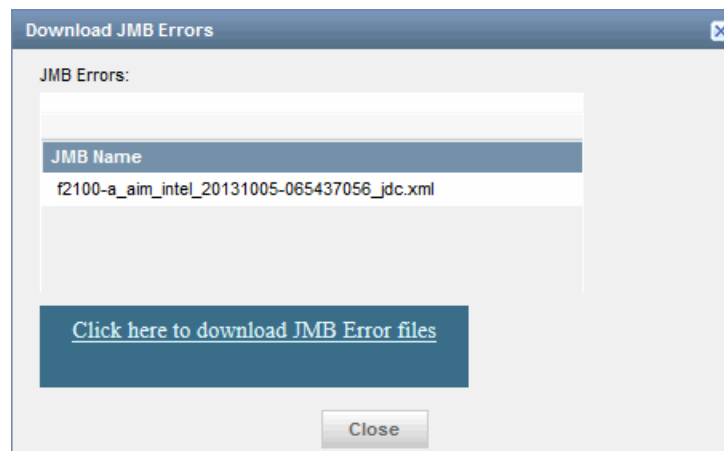
When you download a JMB, it is saved as a zip file. You can download up to five JMBs with errors at a time.

To download JMBs with errors:

1. From the Service Now navigation tree, select **Service Central > JMB Errors**.
The JMB Errors page appears.
2. On the JMB Errors page, select the JMBs that you want to download.
3. From the Actions menu, select **Download JMB Errors**. Alternatively, right-click the selected JMBs and select **Download JMB Errors**.

The Download JMB Errors dialog box appears as shown in [Figure 30 on page 100](#).

Figure 30: Download JMB Errors Dialog Box



4. Click the **Click here to download JMB Error files** link to save the selected JMBs with errors.

Your browser opens a dialog box prompting you to open or save the zip file.

5. Select **Save** to save the file on your local system.
6. Click **OK**.

A dialog box appears to allow you to browse the location where you want to save the file.

7. Click **Save**.

The file is saved on your local system.

Deleting JMBs with Errors

You can delete multiple JMBs with errors at the same time.

To delete JMBs with errors:

1. From the Service Now navigation tree, select **Service Central > Incidents > JMB Errors**.
The JMB Errors page appears.
2. On the JMB Errors page, select one or more JMBs that you want to delete.
3. From the Actions menu, select **Delete**. Alternatively, right-click and select **Delete**.
The Delete Error JMB dialog box prompts you to confirm the deletion.
4. Click **Delete**.

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

- Related Documentation**
- [Service Central Overview on page 32](#)
 - [Messages Overview on page 67](#)

CHAPTER 10

Managing Notifications

- [Notification Policies Overview on page 101](#)
- [Creating and Editing a Notification Policy on page 103](#)
- [Enabling or Disabling a Notification Policy on page 111](#)
- [Deleting a Notification Policy on page 111](#)

Notification Policies Overview

Service Now sends a notification to users when a specific event occurs. Notification policies define the parameters for these notifications. A notification policy specifies the events on Service Now for which you want Service Now to send a notification. It also specifies the actions a user must take for that event.

You must specify the following parameters when you create a notification policy:

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

[Table 14 on page 101](#) lists the triggers and filters that can be configured on Service Now.

Table 14: Notification Triggers and Trigger Filters

Trigger	Description	Filters
New Incident Detected	Trigger to send a notification when a new incident is received from a Service Now Device. This is the only option available when Service Now is in offline mode.	Priority, Organization, Device groups, Device name, Serial number, Has the words, and Does not have
Incident Submitted	Trigger to send a notification when an incident is submitted to JSS for creating a case	Priority, Organization, Device group, Device name, Serial number, Has the words, and Does not have

Table 14: Notification Triggers and Trigger Filters (*continued*)

Trigger	Description	Filters
Case ID Assigned	Trigger to send a notification when a case ID is assigned to an incident in Juniper Support System (JSS)	Priority, Organization, Device groups, Device name, Serial number, Has the words, and Does not have
Case Status Updated	Trigger to send a notification when the status of a case is updated	Priority, Organization, Device groups, Device name, Serial number, Has the words, and Does not have
New Intelligence Update	Trigger to send a notification when one or more device snapshots or informational JMBs are received	Intelligence update type, Products affected, Platform type, Keywords, Serial Number, Software Version, Organization, Device Group, Devices impacted, Has the words, Does not have
Service Contract Expiring	<p>Trigger to send a notification when the technical support contract license is nearing expiry for one or more devices</p> <p>The notification is sent sixty days before expiry of the service contract and lists devices for which the technical support contract is nearing expiry</p>	Organization, Device group, Device name, Serial number
New Exposure	Trigger to send a notification when one or more managed devices are susceptible to known issues	Organization, Device group, Devices
Ship-to Address Missing For Device	Trigger to send a notification when an RMA incident is submitted to Juniper Support Systems without ship-to address	Priority, Organization, Device group, Device name, Serial number, Has the words, Does not have
Switch over enabled for iJMB	<p>Trigger to send a notification when Service Now switches over to auto collection mode for collecting iJMBs (Device Snapshot) for one or more managed devices</p> <p>Service Now switches iJMB collection to auto collection mode when it does not receive iJMBs even though AI-Scripts is installed on the device.</p>	Organization, Device group, Device name, Serial number, Products, Platform type
PHD Collection Failure	Trigger to send a notification when Service Now fails to collect product health data (PHD) from one or more managed devices	Organization, Device group, Device name, Serial number, Send email for every
Connected Member Device Added/Removed	Trigger to send a notification by a Service Now operating in Partner Proxy mode when a device is added or removed by an end customer	Connected member, Device name, Serial number, State

From the Notifications page, you can perform the following actions:

- Edit filters and actions configured for a trigger; see [“Creating and Editing a Notification Policy” on page 103](#) for details.
- Enable or disable a notification policy; see [“Enabling or Disabling a Notification Policy” on page 111](#) for details.

- Delete a notification policy; see [“Deleting a Notification Policy” on page 111](#) for details.

**Related
Documentation**

- [Incidents Overview on page 37](#)
- [Technical and End Customer Support Cases Overview on page 59](#)
- [Messages Overview on page 67](#)
- [Device Snapshots Overview on page 73](#)
- [BIOS Validation Overview on page 79](#)
- [Product Health Data Collection Overview on page 85](#)
- [E-mail Templates Overview](#)

Creating and Editing a Notification Policy

Notification policies specify when you want Service Now to send notifications about an event and the recipients of the notifications. 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 to take after the event is triggered.

To create a notification policy:

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

The Create Notifications page appears as shown in [Figure 31 on page 104](#),

Figure 31: Create Notifications Page

2. Enter a notification policy name, and select a trigger.

The name must be unique and can contain alphanumeric characters, space, hyphen (-), and underscore (_). The maximum number of characters allowed is 64.

3. Expand the Apply Filters section, if not already expanded, and 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 Notifications** dialog box, see [Table 15 on page 105](#).

5. Specify the destinations where SNMP traps can be sent when an event occurs in the **Send SNMP Traps to** section.

For more information about the fields in the **Create Notifications** dialog box, see [Table 15 on page 105](#).

6. Select the **Send JMB file as attachment in mail** check box if the JMB is to be attached to the notification e-mail.

7. Click **Add**.

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

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 navigation tree, select **Service Central > Notifications**.
The Notifications page appears.
2. Select the notification policy that you want to copy, and select **Copy** from either the **Actions** list or the right-click menu.
The Copy Notifications page appears.
3. Make your modifications.
4. Click **Make a Copy**.

A notification policy is created with the settings that you specified and listed in the Notifications page.

To modify a notification policy:

1. From the Service Now navigation tree, select **Service Central > Notifications**.
The Notifications page appears.
2. Select the notification policy that you want to edit, and select **Edit filters and Actions** from either the **Actions** list or the right-click menu.
The Edit Notifications page appears.
3. Edit the desired fields. For more information, see [Table 15 on page 105](#).

Table 15: Create Notification Policy Page Field Descriptions

Field	Description	Range/Length	Remark
Name	Enter a unique name for the policy.	64 characters	—

Table 15: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
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.	New Incident Detected	This is the only option available when Service Now is in offline mode.
		Incident Submitted	
		Case ID Assigned	
		Case Status Updated	
		New Intelligence Update	
		Service Contract Expiring	
		New Exposure	
		Ship-to Address Missing For Device	If this notification is enabled, Service Now will send notification when RMA cases get submitted without the address getting associated to it.
		Switch over enabled for IJMB	If this notification is enabled, the switch over e-mail/SNMPtraps will be sent as per the policy configured. If this policy is not configured, only e-mail will be sent to the Service Now admins configured in space.
		Partner Certificate Expiry	Notifications are sent when the SSL certificate of the partner is about to expire.

Table 15: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
		Connected Member Device Added/Removed	Notification added in Partner Proxy Service Now for devices added or removed by a connected member.

Apply Filters:

NOTE: You can select either Organization or Device Group when creating or modifying a notification.

Filter Parameters for New Incident Detected, Incident Submitted, Case ID Assigned, Case Status Updated and Ship-to Address Missing Triggers:

Priority	Select a value in the Priority field. Service Now sends a notification if the priority of the incident matches the entered value.	255 characters	Blank
Organization	Select a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.	255 characters	Blank
Device Group	Select a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.	255 characters	Blank
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.	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.	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.	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.	255 characters	Blank

Filter Parameters for New Intelligence Update Triggers:

Table 15: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
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.	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
Organization	Enter a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.		
Device Group	Enter a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.		
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.	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.	255 characters	Blank
Filter Parameters for Service Contract Expiring Triggers:			
Organization	Enter a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.		

Table 15: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
Device Group	Enter a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.		
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.	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.	255 characters	Blank
Filter Parameters for New Exposure Triggers:			
Organization	Enter a value in the Organization field. Service Now sends a notification if the organization of the device the incident occurred on matches the entered value.		
Device Group	Enter a value in the Device Group field. Service Now sends a notification if the device group the incident occurred on matches the entered value.		
Devices	Enter a value in the Devices field. Service Now sends a notification if the name of the device the incident occurred on matches the entered value.	255 characters	Blank
Filter Parameters for BIOS Information Updates Trigger:			
Organization	Service Now sends a notification if the organization associated with the device the incident occurred on matches the value entered in this field.		
Device Group	Service Now sends a notification if the device group associated with the device the incident occurred on matches the value entered in this field.		
Device Name	Service Now sends a notification if the name of the device the incident occurred on matches the value entered in this field.		
Serial Number	Service Now sends a notification if the serial number of the device the incident occurred on matches the value entered in this field.		

Table 15: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
BIOS Status	<p>Select a value for the BIOS status. BIOS status indicates the status of BIOS validation.</p> <p>Service Now sends a notification if the BIOS status matches the value selected in this field.</p>	<ul style="list-style-type: none"> Both—a notification is sent irrespective of whether the BIOS validation succeeds or fails. Success—a notification is sent only if the BIOS validation succeeds. Failure—a notification is sent only if the BIOS validation fails. 	
Filter Parameters for PHD Collection Failure Trigger:			
Organization	<p>Select an organization from the drop-down list.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device belonging to the organization.</p>		
Device Group	<p>Select a device group from the drop-down list.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device belonging to the device group.</p>		
Device Name	<p>Enter a device name.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device with the entered device name.</p>		
Serial Number	<p>Enter a serial number.</p> <p>Service Now sends a notification when it fails to collect PHD files from a device with the entered serial number.</p>		
Send Email for every	<p>Select a value from the drop-down list.</p> <p>Service Now send a notification when it fails to collect PHD files from a device for the selected number of hours.</p>	<ul style="list-style-type: none"> 1 Hour 6 Hours 12 Hours 24 Hours 	The default value is 6 hours.
Actions:			
Send Email to	<p>Specify the e-mail addresses of users who must receive an alert if the policy is triggered and matches 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

Table 15: Create Notification Policy Page Field Descriptions (*continued*)

Field	Description	Range/Length	Remark
Send Traps to	Specify the destinations where SNMP traps can be sent when an event occurs and matches the specified filter. See <i>Adding an SNMP Configuration to Service Now</i> .	–	–

- Related Documentation**
- [Notification Policies Overview on page 101](#)
 - [Enabling or Disabling a Notification Policy on page 111](#)
 - [Deleting a Notification Policy on page 111](#)

Enabling or Disabling a Notification Policy

Notification policies specify the events for which Service Now sends notifications, as well as 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 navigation tree, select **Service Central > Notifications**.

The Notifications page appears.

2. Select the notification policies that you want to enable or disable, and select **Enable/Disable** from either the **Actions** list or the right-click menu.

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

3. Click **Change Status** to confirm your action.

The status of the notification policy is changed.

- Related Documentation**
- [Notification Policies Overview on page 101](#)
 - [Creating and Editing a Notification Policy on page 103](#)
 - [Deleting a Notification Policy on page 111](#)
 -

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 navigation tree, select **Service Central > Notifications**.

The Notifications page appears.

2. Select the notification policy that you want to delete, and select **Delete** from either the **Actions** list or the right-click menu.

The **Confirm Deletion of Notification Policies** dialog box displays the name of the notification policy and its owner.

3. Click **Delete**.

This action deletes the selected notification policies from the Service Now database and from the Notifications page.

**Related
Documentation**

- [Notification Policies Overview on page 101](#)
- [Creating and Editing a Notification Policy on page 103](#)
- [Enabling or Disabling a Notification Policy on page 111](#)

CHAPTER 11

Trouble Ticketing

- [Setting up Java Based Web Service Client on page 113](#)
- [Accessing a Web Service on page 118](#)

Setting up Java Based Web Service Client

To set up a java based web service client:

1. Download the WSDL and XSD files from Service Now server [https://IP address/aimOSSTroubleTicketService/OSSJWSDLFile?baseURL=https://\[IP Address\]/aimOSSTroubleTicketService/JVTTroubleTicketWS](https://IP address/aimOSSTroubleTicketService/OSSJWSDLFile?baseURL=https://[IP Address]/aimOSSTroubleTicketService/JVTTroubleTicketWS) , where *IP address* is the IP address of the Service Now host.
2. Download the OSSJWSDLAndXSDFiles.zip file containing the WSDL and XSD files. Extract the zip files to the required location.

The zip file contains the following files:

- JVTTroubleTicketSession.wsdl
- WS-BaseNotification.wsdl
- WS-Resource.wsdl
- License.xml
- xsd/notification/b-2.xsd
- xsd/notification/bf-2.xsd
- xsd/notification/r-2.xsd
- xsd/notification/t-1.xsd
- xsd/notification/ws-addr.xsd
- troubleTicket/OSSJ-Common-v1-5.xsd
- troubleTicket/OSSJ-Common-CBEBi-v1-5.xsd
- troubleTicket/OSSJ-Common-CBECORE-v1-5.xsd
- troubleTicket/OSSJ-Common-CBEDatatypes-v1-5.xsd
- troubleTicket/OSSJ-Common-CBELocation-v1-5.xsd

- troubleTicket/OSSJ-Common-CBEParty-v1-5.xsd
 - troubleTicket/OSSJ-Common-SharedAlarm-v1-5.xsd
 - troubleTicket/OSSJ-TroubleTicket-CBETrouble-v1-2.xsd
 - troubleTicket/OSSJ-TroubleTicket-v1-2.xsd
 - troubleTicket/OSSJ-TroubleTicket_x790-v0-5.xsd
3. In a windows system, select **START** > **RUN** to open the command prompt. Type **cmd** in the Run dialog box, and then press **OK**. Navigate to the location where the zip file has been extracted.
 4. Navigate to the location where the zip file is extracted and run the following command to generate the service Now OSS/J web service client binaries: **wsimport -d [LOCATION_FOR_CLIENT_BINARIES] JVTTroubleTicketSession.wsdl**. where *LOCATION_FOR_CLIENT_BINARIES* is the location to generate the web service client.

Example— OSSJTroubleTicketClient.java:

```
import java.lang.reflect.Field;
import java.lang.reflect.InvocationTargetException;
import java.lang.reflect.Method;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import java.util.ArrayList;
import java.util.List;

import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import javax.xml.bind.JAXBElement;
import javax.xml.ws.BindingProvider;
import javax.xml.ws.handler.Handler;

import org.apache.xerces.jaxp.datatype.DatatypeFactoryImpl;
import org.ossj.wsdl.troubleticket.v1_2.JVTTroubleTicketSessionWSPort;
import org.ossj.wsdl.troubleticket.v1_2.JVTTroubleTicketSessionWebService;
import org.ossj.xml.common.ArrayOfString;
import org.ossj.xml.troubleticket.v1_2.*;

public class OSSJTroubleTicketClient {

    public static void main(String[] args) {
        try {

            //create web service client object
            JVTTroubleTicketSessionWebService webService1 = new

                                JVTTroubleTicketSessionWebService();
            //get the port from the webservice client

            JVTTroubleTicketSessionWSPort port =
```

```

webService1.getJVTTroubleTicketSessionWSPort();
//disable SSL certificate verification - this will be needed when using HTTPS server.
disableCertificateValidation();

//Authentication data must be added into SOAP request, for this creating a handler
//chain which adds the authentication in SOAP header of the outgoing message.
//The handler chain is then associated with the webservice port
List<Handler> handlerChain = new ArrayList<Handler>();
handlerChain.add(new SOAPLoggingHandler());
BindingProvider bindingProvider = (BindingProvider) port;
List<javax.xml.ws.handler.Handler> ls =
    bindingProvider.getBinding().getHandlerChain();
ls.add(new SOAPLoggingHandler());
bindingProvider.getBinding().setHandlerChain(handlerChain);

//create request for creating trouble ticket
CreateTroubleTicketByValueRequest request = createTroubleTicketValueRequest();

//invoke the createTroubleTicketByValue API
CreateTroubleTicketByValueResponse response =
port.createTroubleTicketByValue(request);

} catch (Exception e) {
    e.printStackTrace();
}
}

public static void disableCertificateValidation() {
// Create a trust manager that does not validate certificate chains
TrustManager[] trustAllCerts = new TrustManager[] {
    new X509TrustManager() {
        public X509Certificate[] getAcceptedIssuers() {
            return new X509Certificate[0];
        }
        public void checkClientTrusted(X509Certificate[] certs, String authType) {}
        public void checkServerTrusted(X509Certificate[] certs, String authType) {}
    }
};
// Ignore differences between given hostname and certificate hostname
HostnameVerifier hv = new HostnameVerifier() {
    public boolean verify(String hostname, SSLSession session) { return true; }
};

// Install the all-trusting trust manager
try {
    SSLContext sc = SSLContext.getInstance("SSL");
    sc.init(null, trustAllCerts, new SecureRandom());
    HttpsURLConnection.setDefaultSSLSocketFactory(sc.getSocketFactory());
    HttpsURLConnection.setDefaultHostnameVerifier(hv);
} catch (Exception e) {}
}

private static CreateTroubleTicketByValueRequest createTroubleTicketValueRequest()

```

```
{  
  
    TroubleTicketValue value = new ObjectFactory().createTroubleTicketValue();  
  
    //set the values in TroubleTicketValue object  
  
        CreateTroubleTicketByValueRequest request = new  
            ObjectFactory().createCreateTroubleTicketByValueRequest();  
  
    request.setTroubleTicketValue(value);  
  
    return request;  
    }  
}
```

Example—SOAPLoggingHandler.java

```
import java.io.ByteArrayOutputStream;  
import java.util.Set;  
import java.util.logging.Logger;  
  
import javax.xml.namespace.QName;  
import javax.xml.soap.SOAPElement;  
import javax.xml.soap.SOAPException;  
import javax.xml.soap.SOAPHeader;  
import javax.xml.soap.SOAPEnvelope;  
import javax.xml.soap.SOAPMessage;  
import javax.xml.ws.handler.MessageContext;  
import javax.xml.ws.handler.soap.SOAPHandler;  
import javax.xml.ws.handler.soap.SOAPMessageContext;  
  
public class SOAPLoggingHandler implements SOAPHandler<SOAPMessageContext>  
{  
    private static Logger logger =  
        Logger.getLogger(SOAPLoggingHandler.class.getName());  
  
    public boolean handleMessage(SOAPMessageContext context) {  
        Boolean outgoingMsg = (Boolean)  
            context.get(MessageContext.MESSAGE_OUTBOUND_PROPERTY);  
        SOAPMessage soapMsg = context.getMessage();  
  
        if(soapMsg != null && soapMsg.getSOAPPart() != null) {  
  
            SOAPEnvelope soapEnv;  
  
            try {  
                soapEnv = soapMsg.getSOAPPart().getEnvelope();  
                SOAPHeader soapHeader = soapEnv.getHeader();  
                if (soapHeader == null) {  
                    soapHeader = soapEnv.addHeader();  
                }  
            }  
        }  
    }  
}
```

```

addAuthentication(soapHeader);
    } catch (SOAPException e) {
    // TODO Auto-generated catch block
    e.printStackTrace();
    }
}

if (outGoingMsg)
    System.out.println("#####outgoing soap message#####");
else
    System.out.println("#####incoming soap message#####");

    logSoapMessage(context);

    return true;
}

public boolean handleFault(SOAPMessageContext context) {

    System.out.println("#####Fault soap message#####");
    logSoapMessage(context);

return true;
}

public void close(MessageContext context) {

}

public void logSoapMessage(SOAPMessageContext context) {

    try {
        SOAPMessage msg = context.getMessage();

        ByteArrayOutputStream bas = new ByteArrayOutputStream();
        msg.writeTo(bas);
        System.out.println(bas);
    }
    catch (Exception e) {
        System.out.println("Error while writing SOAP message to debug log " + e);
    }
}

public Set<QName> getHeaders() {
    return null;
}
private void addAuthentication(SOAPHeader header) {
    try {

        SOAPElement security =
            header.addChildElement("Security", "wsse", "http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd");

        SOAPElement usernameToken =
            security.addChildElement("UsernameToken", "wsse",
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd");

```

```
SOAPElement username =
    usernameToken.addChildElement("Username", "wsse");
username.addTextNode("****");

SOAPElement password =
    usernameToken.addChildElement("Password", "wsse");
password.setAttribute("Type",
"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText");

password.addTextNode("****");

} catch (Exception e) {
    e.printStackTrace();
}

}

}
```

**Related
Documentation**

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Overview on page 121](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Accessing a Web Service on page 118](#)
- [Profiles Used by Service Now on page 122](#)
- [Error Messages Displayed by OSS/J Client on page 127](#)

Accessing a Web Service

Access to a Web Service (WS) or a OSS/J Trouble Ticket (TT) API requires authentication. An OSS/J Client has to use a user name and password of Junos Space server when making calls through the OSS/J TT API to create and modify tickets on the trouble ticket management system.

The procedure to access web service is as follows:

1. The OSS/J client adds the authentication details in the SOAP header of a WS request.
2. The client requests are intercepted by JAX-WS handlers at WS server for getting authenticated.
3. JAX-WS handler parse the SOAP header to get the authentication details.

4. The username and password are authenticated by making REST call to Junos Space. If the authentication is successful, the web service request is forwarded to JVT profile to invoke the appropriate internal rest call to Service Now API.
5. The SOAPFault exception is thrown if authentication fails.

The Web Service messages comply with the WS_SECURITY standard. A dedicated security header defines properties for user and password that must be added.

Soap Header Template

```
<soapenv:Header>

<wsse:Security soapenv:mustUnderstand="0"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd"><wsse:UsernameToken
wsse:Id="UsernameToken-14327075"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"><wsse:Username>***</wsse:Username><wsse:Password
Type="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordText">***</wsse:Password></wsse:UsernameToken></wsse:Security>

</soapenv:Header>
```

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Overview on page 121](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Setting up Java Based Web Service Client on page 113](#)
- [Profiles Used by Service Now on page 122](#)
- [Error Messages Displayed by OSS/J Client on page 127](#)

CHAPTER 12

Trouble Ticket API

- [Trouble Ticket APIs Overview on page 121](#)
- [Profiles Used by Service Now on page 122](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Error Messages Displayed by OSS/J Client on page 127](#)

Trouble Ticket APIs Overview

Service Now supports trouble ticket APIs that allow you to perform the following functions:

- Create, query, close, or cancel trouble tickets (single/multiple)
- Change the values of trouble tickets (single/multiple)
- Obtain notification regarding ticket changes

The Operation Support Systems for Java (OSS/J) delivers standards-based interface implementations (OSS/J APIs) and design guidelines for the development of component-based OSS systems. The web service technology is used to expose the standard set of APIs defined under JSR91 of OSS/J. The OSS/J module is integrated into Service Now. For more details, refer to the JSR 91 specification at <http://www.tmforum.org>.

The version of the trouble ticket supported by Service Now is TroubleTicket_x790/v0-5.

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Setting up Java Based Web Service Client on page 113](#)
- [Profiles Used by Service Now on page 122](#)
- [Accessing a Web Service on page 118](#)
- [Error Messages Displayed by OSS/J Client on page 127](#)

Profiles Used by Service Now

A profile in OSS through Java is equivalent to an interaction pattern. A profile describes how a client can interact with the OSS/J application.

Currently, Service Now supports the Web Services style interaction profile (WSIP) for displaying trouble ticket APIs to clients. The reason for choosing Web Services is its ability to enable different systems to communicate at the protocol level without requiring any specific agreement on middleware, software libraries, programming languages, component models, application server platforms, processors or operating systems.

WSIP relies on well established standards such as SOAP (Simple Object Access Protocol) and WSDL (Web Services Description Language).

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Overview on page 121](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Setting up Java Based Web Service Client on page 113](#)
- [Accessing a Web Service on page 118](#)
- [Error Messages Displayed by OSS/J Client on page 127](#)

Trouble Ticket APIs Supported by Service Now

The client provides operations (getting, creating, changing or canceling/closing tickets) to manage and retrieve trouble tickets from the trouble ticket management system.

The following list of APIs from JSR91 specification are implemented in Service Now.

- createTroubleTicketByValue
- tryCreateTroubleTicketsByValues
- getTroubleTicketByKey
- getTroubleTicketsByKeys
- setTroubleTicketByValue
- trySetTroubleTicketsByValues
- trySetTroubleTicketsByKeys
- tryCancelTroubleTicketsByKeys
- tryCloseTroubleTicketsByKeys
- cancelTroubleTicketByKey

- `closeTroubleTicketByKey`
- `getTroubleTicketTypes`
- `getEventTypes`
- `getEventDescriptor`
- `getManagedEntityType`
- `getSupportedOptionalOperations`

The following table describes the trouble ticket APIs.

Table 16: Trouble Ticket APIs Supported by Service Now

Troube Ticket API	Description
<code>createTroubleTicketByValue</code>	Creates a single trouble ticket
<code>tryCreateTroubleTicketsByValues</code>	Creates multiple trouble tickets
<code>getTroubleTicketByKey</code>	Obtains a single trouble ticket using the given key and returns only the requested attributes
<code>getTroubleTicketsByKeys</code>	Obtains multiple trouble tickets using the given keys and returns only the requested attributes
<code>setTroubleTicketByValue</code>	Updates a single trouble ticket using the given value
<code>trySetTroubleTicketsByValues</code>	Best effort update of multiple trouble ticket items by the given values
<code>trySetTroubleTicketsByKeys</code>	Best effort update of multiple trouble ticket items by the given keys
<code>tryCancelTroubleTicketsByKeys</code>	Cancels multiple trouble tickets indicated by the given keys
<code>tryCloseTroubleTicketsByKeys</code>	Best effort closing of multiple trouble tickets indicated by the given keys
<code>cancelTroubleTicketByKey</code>	Cancels a trouble ticket indicated by the given key
<code>closeTroubleTicketByKey</code>	Closes a trouble ticket indicated by the given key

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Overview on page 121](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Setting up Java Based Web Service Client on page 113](#)
- [Profiles Used by Service Now on page 122](#)
- [Accessing a Web Service on page 118](#)
- [Error Messages Displayed by OSS/J Client on page 127](#)

Trouble Ticket Attributes Supported by Service Now

The following table lists the attributes supported by Service Now.

Table 17: Supported Trouble Ticket Attributes

Trouble Ticket Attribute	Description	Access Right Provided to an External System
troubleTicketKey	Unique key to identify a trouble ticket.	Read access
additionalTroubleInfoList	Describes the reported trouble. It is represented by a set of graphic strings.	Read/write/access
attachmentData	Contains filename and data. The size of the data can be 6 MB (maximum) per attachment Base64 encoded. Attachments can be updated/added through update/create trouble ticket. If file name is not displayed, it is derived from the data. It will be assumed the name of the file in the attachment data will be the name of the file. If the attachment data has no file name, the attachment data will be given an arbitrary file name as attachment_1 and so on.	Only upload access
closeOutNarr	Provides additional information regarding the trouble report closure.	Read/write access
relatedTroubleTicketKeyList	Provides a list of related TRs.	Read access
troubleDescription	Provides a summary of the PR.	Write access is provided only at the first attempt. For all subsequent updates, only read access is provided.
baseState	Indicates the state of a ticket/case.	Read/write access
baseStatus	Indicates the status of a ticket/case	Read/write access
troubleDetectionTime	Indicates when the trouble was detected.	Read/write access
cancelRequestedByCustomer	Indicates whether the customer has requested to cancel the case. Cancellation request is not permitted if the case is already cleared or closed. The case is closed when a cancellation request is granted.	Write access
closeOutVerification	Indicates whether the customer has verified the resolution, denied the resolution, or taken no action.	Write access

Table 17: Supported Trouble Ticket Attributes (*continued*)

Trouble Ticket Attribute	Description	Access Right Provided to an External System
customerTroubleNum	Specifies the internal number assigned to the customer (example, the number that is assigned by a customer's trouble administration system). It allows the customer to access the TTR with this internal number.	Read/write access
basePreferredPriority	Specifies the urgency of the resolution required by the customer. Its value can be undefined, minor, major, or serious.	Read/write access
SuspectObjectList	Provides the list of objects that may be the underlying cause of the trouble. This list should be used to pass the device serial number.	Read/write access

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Overview on page 121](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Setting up Java Based Web Service Client on page 113](#)
- [Profiles Used by Service Now on page 122](#)
- [Accessing a Web Service on page 118](#)
- [Error Messages Displayed by OSS/J Client on page 127](#)

Trouble Ticket Events Supported by Service Now

You can track a trouble ticket or a trouble ticket item that is created, modified or deleted, by means of notifications. Service Now supports the WS-BaseNotification (a standard defined by OASIS) to receive events (notifications).

To receive events through a Web Service, you need to subscribe to the server-side web service. The server-side web service implements administration tasks to manage the subscription. The client-side service implements methods to receive events.

The JSR91 standard events implemented by Service Now are described as follows:

- **TroubleTicketCreateEvent**—The trouble ticket management system publishes this event when a trouble ticket is created. This event must be the first event published for a specific trouble ticket.

Supported attributes: The trouble ticket must contain all the attributes listed in table “[Trouble Ticket Attributes Supported by Service Now](#)” on page 124. The trouble ticket must contain a value for the trouble ticket key to identify the trouble ticket.

- **TroubleTicketAttributeValueChangeEvent**—The trouble ticket management system publishes this event when the value of a trouble ticket attribute is modified. This includes update, closure or cancellation of a trouble ticket as well as changes during the execution of a trouble ticket.

Supported attributes: This event includes all the attributes listed in “[Trouble Ticket Attributes Supported by Service Now](#)” on page 124. This event is published when a trouble ticket item is associated to or disassociated from a trouble ticket and also when the baseState or the baseStatus attributes are modified. This event must contain a value for the troubleTicketValue attribute and the value must contain all new values of the modified attributes. Attributes that are not changed are not populated.

- **TroubleTicketStatusChangeEvent**—The trouble ticket management system publishes this event when the status of a trouble ticket is changed. When the status of the trouble ticket changes, both TroubleTicketAttributeValueChangeEvent and TroubleTicketStatusChangeEvent are published. This event is published when the values of the baseState and the baseStatus attributes are modified.

Supported attributes: The event contains the mandatory attribute troubleTicketKey that holds the key value of the affected trouble ticket, and the baseState and the baseStatus attributes that hold the state value of the new trouble ticket.

- **TroubleTicketCloseOutEvent**—The trouble ticket management system publishes this event when a trouble ticket is closed.

Supported attributes: This event extends the event type TroubleTicketStatusChangeEvent and thus contains the same attributes used in TroubleTicketStatusChangeEvent, and is used in the same method as TroubleTicketStatusChangeEvent. The mandatory attributes baseState and baseStatus contain the new values. The other attribute value of a trouble ticket contains the history information of the closed trouble ticket. This includes the change of state due to a closed or an updated operation as well as changes during the execution of a trouble ticket implementation.

Related Documentation

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Overview on page 121](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Setting up Java Based Web Service Client on page 113](#)
- [Profiles Used by Service Now on page 122](#)
- [Accessing a Web Service on page 118](#)

- [Error Messages Displayed by OSS/J Client on page 127](#)

Error Messages Displayed by OSS/J Client

The error descriptions and the supported APIs for the various error scenarios are given as follows:

Table 18: OSS/J Client Error Scenarios

OSSJ Error Description	Supported APIs
JNPRERROR-998: Username and/or password are/is not valid in Space. Please check your entries in Space and resubmit your request. If the problem persists, please contact Juniper Customer Support.	All APIs
JNPRERROR-1020: Organization is not configured in Service Now. Please check your entries in Service Now and resubmit your request. If the problem persists, please contact Juniper Customer Support.	All APIs
JNPRERROR-1005: Juniper system is unresponsive at this moment. Please try again later. If the problem persists, please contact Juniper Customer Support.	All APIs
JNPRERROR-1014: There is already an active Trouble Ticket for the supplied serial number, product, platform and trouble description combination. Trouble Ticket Id: 2013-0617-1021. Please use this Trouble Ticket Id if you wish to provide any additional information or updates to this issue.	createTroubleTicketByValue createTroubleTicketByValue
JNPRERROR-1013: Trouble Ticket Id 2013-0617-1022 in Juniper System is already Closed or Cancelled and cannot be updated. Please request for a new ticket through appropriate messaging.	setTroubleTicketByValue trySetTroubleTicketsByValues trySetTroubleTicketsByKeys tryCancelTroubleTicketsByKeys tryCloseTroubleTicketsByKeys cancelTroubleTicketByKey closeTroubleTicketByKey
JNPRERROR-1012: Juniper System could not validate the support entitlement for the supplied device 0000233004A. Please contact Juniper Customer Support to verify the support eligibility of the device.	createTroubleTicketByValue tryCreateTroubleTicketsByValues

Table 18: OSS/J Client Error Scenarios (*continued*)

OSSJ Error Description	Supported APIs
JNPRWARN-1002: Product details like series and platform could not be determined from the information supplied in the Trouble Ticket. So an admin trouble ticket is created in Juniper System and assigned to Juniper Customer Care who is soon going to contact you to obtain relevant details before the Trouble Ticket can be assigned to the right Technical Engineer to troubleshoot the problem.	createTroubleTicketByValue tryCreateTroubleTicketsByValues
JNPRERROR-1027: Cannot create Trouble Ticket as Trouble Description, Trouble Detection Time, Suspect Object Id is null or empty. Trouble Description, Trouble Detection Time and Suspect Object Id are mandatory parameters for creating a Trouble Ticket. Please provide a valid input and resubmit your request.	createTroubleTicketByValue tryCreateTroubleTicketsByValues
JNPRERROR-1000: An unexpected error has occurred in the Juniper Backend System. Please try again later. If the problem persists, please contact Juniper Customer Support.	All APIs
JNPRERROR-1021: Base State of a Trouble Ticket can only be OPEN, ACTIVE or QUEUED while creating a Trouble Ticket. Please provide a valid Base State and resubmit your request.	createTroubleTicketByValue tryCreateTroubleTicketsByValues
JNPRERROR-1018: Cannot create or update Trouble Ticket as Customer Trouble Number is greater than 40 characters. Please provide a valid Customer Trouble Number that Service Now understands to create or update a Trouble Ticket.	createTroubleTicketByValue tryCreateTroubleTicketsByValues setTroubleTicketByValue trySetTroubleTicketsByValues trySetTroubleTicketsByKeys
JNPRERROR-1023: Primary key of a Trouble Ticket should not be null or empty while fetching or updating a Trouble Ticket. Please provide a valid Trouble Ticket Primary Key and resubmit your request.	getTroubleTicketByKey getTroubleTicketsByKeys setTroubleTicketByValue trySetTroubleTicketsByValues trySetTroubleTicketsByKeys tryCancelTroubleTicketsByKeys tryCloseTroubleTicketsByKeys cancelTroubleTicketByKey closeTroubleTicketByKey
JNPRERROR-999: [method name] API is not supported in OSS/J implementation of Service Now.	APIs that are not supported by Service Now implementation of JSR91.

**Related
Documentation**

- [Junos Space Service Now Overview on page 17](#)
- [Trouble Ticket APIs Overview on page 121](#)
- [Trouble Ticket APIs Supported by Service Now on page 122](#)
- [Trouble Ticket Attributes Supported by Service Now on page 124](#)
- [Trouble Ticket Events Supported by Service Now on page 125](#)
- [Setting up Java Based Web Service Client on page 113](#)
- [Accessing a Web Service on page 118](#)
- [Profiles Used by Service Now on page 122](#)

CHAPTER 13

Index

- [Index on page 133](#)

Index

Symbols

#, comments in configuration statements.....	xiii
(), in syntax descriptions.....	xiii
< >, in syntax descriptions.....	xiii
[], in configuration statements.....	xiii
{ }, in configuration statements.....	xiii
(pipe), in syntax descriptions.....	xiii

B

braces, in configuration statements.....	xiii
brackets	
angle, in syntax descriptions.....	xiii
square, in configuration statements.....	xiii

C

comments, in configuration statements.....	xiii
conventions	
text and syntax.....	xii
curly braces, in configuration statements.....	xiii
customer support.....	xiv
contacting JTAC.....	xiv

D

dashboard overview	
Dashboard Gadgets.....	30
Service Now Workspaces.....	29
deleting	
iJMB.....	77
incident.....	56
information message.....	72
notification policy.....	111
documentation	
comments on.....	xiii

E

export iJMB	
html.....	76

F

font conventions.....	xii
-----------------------	-----

I

incident	
assigning owner.....	42
export to Excel.....	50
flagging.....	48
submitting.....	44
information message	
assign connected member.....	70
assign owner.....	68
flagging.....	68

J

JMB error.....	99
----------------	----

M

manuals	
comments on.....	xiii
modes	
Service Now.....	20

N

notification policy	
create.....	103
enable/disable.....	111

O

overview	
device snapshots.....	73
Incidents.....	37
messages.....	67
notifications.....	101
Service Central	32

P

parentheses, in syntax descriptions.....	xiii
--	------

S

scan iJMB for ipact.....	69
Service Now	
modes.....	20
Service Now Overview.....	17
support, technical See technical support	
syntax conventions.....	xii

T

technical support	
contacting JTAC.....	xiv

V

view

case in Case Manager.....	49
incident details	40
JMB details.....	74