



Junos Space Service Now User Guide

Release

18.1R1



Modified: 2018-12-13

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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

18.1R1

Copyright © 2018 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 <https://support.juniper.net/support/eula/>. 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
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xv
Chapter 1	Junos Space Service Now Overview	17
	Junos Space Service Now Overview	17
	Benefits of Junos Space Service Now	19
	Junos Space Service Now Modes	20
	Service Now MIBs	23
	Service Now Domain Overview	24
	Assigning a Service Now Object to Another Domain	26
	Filtering Inventory Pages on Service Now and Service Insight	27
	Service Now Dashboard Overview	30
	Service Now Workspaces	30
	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
	Service Now Incidents Overview	37
	Associated Actions	39
	Viewing Incident Details	41
	Viewing Knowledge Base Articles Associated with an Incident	43
	Assigning an Owner to an Incident	44
	Submitting an Incident to Juniper Support Systems or Service Now Partner	45
	Flagging an Incident to a User	51
	Exporting a Juniper Message Bundle (JMB) to an HTML file	52
	Updating an End-Customer Case	54
	Uploading an Attachment to an Incident	55
	Uploading Core Files to JSS for an Incident	57
	Checking Incident Status Updates	58
	Deleting an Incident	59
	Associating an Incident with an Existing Case	59

Chapter 4	Managing Cases	63
	Service Now Technical Support Cases and End Customer Support Cases	
	Overview	63
	Associated Actions	66
	Viewing a Case in Case Manager	67
	Updating an End-Customer Case	68
	Uploading an Attachment to a Case	70
Chapter 5	Collecting Additional Information for Incidents and Cases	73
	Collecting Additional Information for Service Now Incidents and Cases	
	Overview	74
	Associated Actions	74
	Configuring Junos OS Commands to Collect Additional Information About an Incident	75
	Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident	78
	Modifying the Settings for Collecting Additional Information for an Incident	79
	Deleting the Settings for Collecting Additional Information for an Incident	81
	Downloading the Additional Information Collected About an Incident	82
	Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case	84
	Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case	85
	Modifying the Configuration for Collecting Additional Information for a Technical Support Case	88
	Deleting the Configuration for Collecting Additional Information for a Technical Support Case	90
	Downloading the Additional Information Collected for a Technical Support Case	91
Chapter 6	Managing Messages	93
	Service Now Messages Overview	93
	Associated Actions	93
	Assigning Ownership to Messages	94
	Flagging a Message to Users	95
	Scanning a Message for Impact	95
	Assigning a Message to an End Customer	96
	Deleting a Message	98
Chapter 7	Managing Device Snapshots or iJMBs	99
	Service Now Device Snapshots Overview	99
	Associated Actions	100
	Viewing Details of a Device Snapshot	100
	Exporting Device Snapshots to HTML	102
	Deleting Device Snapshots	103

Chapter 8	Managing BIOS Validations	105
	Service Now BIOS Validation Overview	105
	Associated Actions	106
	Viewing BIOS Validations	107
	Exporting BIOS Validation Results	109
	Deleting BIOS Validation Incidents	110
Chapter 9	Analyzing Physical Health Data	113
	Service Now Product Health Data Collection Overview	113
	Exporting Product Health Data Information to an Excel File	115
	Exporting Information about Devices on which PHDC is configured	116
	Exporting Data about PHD Files Collected from a Device	118
	Viewing Product Health Data Files Collected from a Device	120
	Deleting Product Health Data Files Collected from a Device	124
Chapter 10	Managing JMB with Errors	127
	JMBs with Errors	127
	Downloading JMBs with Errors	127
	Deleting JMBs with Errors	128
Chapter 11	Viewing and Managing Suppressed Events	131
	Service Now Suppressed Events Overview	131
	Associated Actions	131
	Viewing Details of JMBs for Suppressed Events	132
	Creating Incidents for Suppressed Juniper Message Bundles	132
	Deleting JMBs for Suppressed Events	134
Chapter 12	Managing Notifications	135
	Service Now Notification Policies Overview	135
	Associated Actions	136
	Creating and Editing a Notification Policy	137
	Enabling or Disabling a Notification Policy	146
	Deleting a Notification Policy	146
Chapter 13	Trouble Ticketing	149
	Setting up Java Based Web Service Client	149
	Accessing a Web Service	154
Chapter 14	Trouble Ticket API	157
	Trouble Ticket APIs Overview	157
	Profiles Used by Service Now	158
	Trouble Ticket APIs Supported by Service Now	158
	Trouble Ticket Attributes Supported by Service Now	160
	Trouble Ticket Events Supported by Service Now	161
	Error Messages Displayed by OSS/J Client	163

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	42
	Figure 7: Submit Case Options Page	47
	Figure 8: Export JMB to HTML Dialog Box	53
	Figure 9: End-Customer Cases Dialog Box	54
	Figure 10: Upload Attachment Dialog Box	56
	Figure 11: Associate Case ID Page	60
Chapter 4	Managing Cases	63
	Figure 12: View Tech Support Cases	64
	Figure 13: View End Customer Cases Page	65
	Figure 14: End-Customer Cases Dialog Box	69
	Figure 15: Upload Attachment Dialog Box	71
Chapter 5	Collecting Additional Information for Incidents and Cases	73
	Figure 16: Collect Additional Information Page	76
	Figure 17: Collect Additional Information Jobs Results Summary page	78
	Figure 18: Modify Collect Additional Information page	80
	Figure 19: Cancel Job Dialog Box	82
	Figure 20: Collect Additional Information Attachment Details Tab on the Incident Details Page	83
	Figure 21: Collect Additional Information Jobs Results Summary Page	84
	Figure 22: Collect Additional Information Page	87
	Figure 23: Modify Collect Additional Information Page	89
	Figure 24: Cancel Job Dialog Box	91
Chapter 6	Managing Messages	93
	Figure 25: Choose Connected Members Dialog Box	97
Chapter 7	Managing Device Snapshots or iJMBs	99
	Figure 26: Juniper Message Bundle	101
	Figure 27: View JMB Dialog Box	101
Chapter 8	Managing BIOS Validations	105
	Figure 28: BIOS Validation Legal Notice on Service Now Partner	106
	Figure 29: BIOS Validation Legal Notice on Service Now End Customer	106

Chapter 9	Analyzing Physical Health Data	113
	Figure 30: Product Health Data Devices Page	114
	Figure 31: PHDC Information of Devices Exported to Excel	115
	Figure 32: PHD Files Information Exported to Excel	116
	Figure 33: View all Devices of this PHDC	117
	Figure 34: View All Product Health Data Files Page	119
	Figure 35: View All Devices of this PHDC Page	119
	Figure 36: View All Product Health Data Files Page	121
	Figure 37: View All Devices of this PHDC Page	123
	Figure 38: View All Product Health Data Files Page	125
	Figure 39: View All Devices of this PHDC Page	125
Chapter 10	Managing JMB with Errors	127
	Figure 40: Download JMB Errors Dialog Box	128
Chapter 11	Viewing and Managing Suppressed Events	131
	Figure 41: Suppressed Events Page	131
	Figure 42: Create Incident for Suppressed JMBs Dialog Box	133
	Figure 43: Delete Suppressed Events Dialog Box	134
Chapter 12	Managing Notifications	135
	Figure 44: Create Notifications Page	138

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	28
Chapter 3	Managing Incidents	37
	Table 6: Fields on the Incidents Page	38
Chapter 4	Managing Cases	63
	Table 7: Fields on the View Tech Support Cases Page	64
	Table 8: Fields on the View End Customer Cases Page	66
Chapter 8	Managing BIOS Validations	105
	Table 9: BIOS Validations Field Descriptions	107
	Table 10: BIOS Validation Field Descriptions	109
Chapter 9	Analyzing Physical Health Data	113
	Table 11: Fields on the Product Health Data Devices Page	114
	Table 12: Fields on the View All Product Health Data Files Page	121
Chapter 12	Managing Notifications	135
	Table 13: Notification Triggers and Trigger Filters	135
	Table 14: Create Notification Policy Page Field Descriptions	140
Chapter 14	Trouble Ticket API	157
	Table 15: Trouble Ticket APIs Supported by Service Now	159
	Table 16: Supported Trouble Ticket Attributes	160
	Table 17: OSS/J Client Error Scenarios	163

About the Documentation

- Documentation and Release Notes 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 <https://www.juniper.net/documentation/>.

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 <https://www.juniper.net/books>.

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>

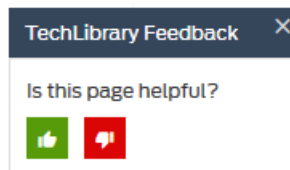
Table 2: Text and Syntax Conventions (continued)

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.	[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

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

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 <https://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 <https://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 Overview on page 24](#)
- [Filtering Inventory Pages on Service Now and Service Insight on page 27](#)
- [Service Now Dashboard Overview on page 30](#)
- [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. Your contract with Juniper Networks determines whether Service Now operates in direct 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 [“Junos Space Service Now Modes” on page 20](#).

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 detects the event and automatically collects diagnostic data and packages the data in an XML file called *Juniper Message Bundle (JMB)*.

For information about AI-Scripts, see *AI-Scripts Overview*.

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 policies (known as auto submit policies) to automatically submit an incident to JSS as soon as the incident is created. Service Now provides options to define the level of information that you share in a JMB 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.
- View device snapshots, BIOS data, and product health data.

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 device snapshots to JSS. 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 group the devices into device groups and 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 manage groups of devices with similar attributes or uses efficiently.

Service Now also sends SNMP traps if notification policies are configured to send traps when events occur on devices. From Service Now and Service Insight Release 14.1R1, 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 30](#).

From Release 14.1R1 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 Now Getting Started 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 Platform and other Junos Space applications are still running. Refer to *Junos Space Service Now User Roles* for information about tasks that can be performed for a user role.

Benefits of Junos Space Service Now

- **Automatic collection of troubleshooting information**—Information, such as system logs, core files, request support information, and so on, required for troubleshooting an event is automatically collected by AI-Scripts and submitted to Service Now.
- **Automatic submission of incidents and troubleshooting information to JSS**—Auto submit policies configured on Service Now help you to submit the details of issues that occurred on a device and the associated troubleshooting information to JSS to create a case, significantly reducing time and effort to resolve the issue.
- **Ensure optimal health of managed devices**—Device snapshots, BIOS validations, and product health data collection features help you proactively identify potential risks with your devices and mitigate any network downtime due to the risks.

Related Documentation

- *Service Now Administration Workspace Overview*
- [Service Automation Implementation Guide](#)

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 Systems (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 or Service Now partner 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 manage 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.

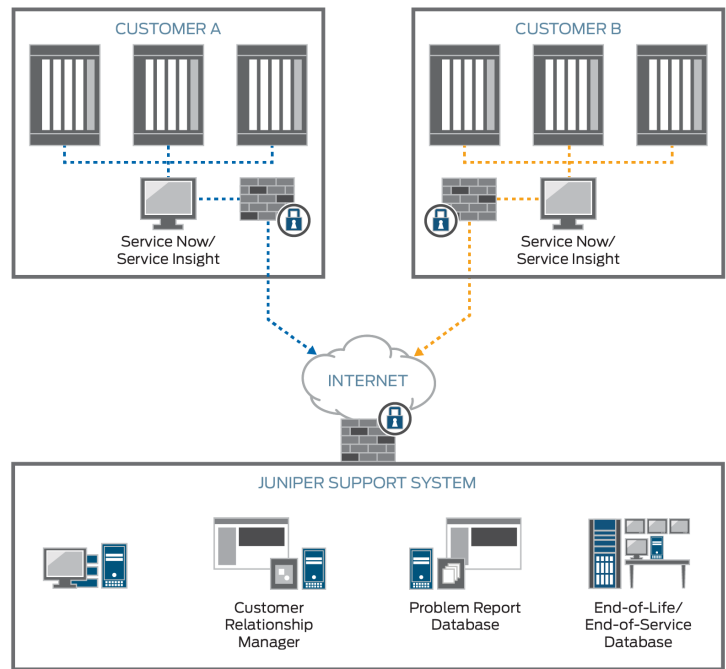


NOTE: If Service Now is already in End Customer mode, you cannot operate it in Offline mode.

- Direct mode—In Direct mode, you can add multiple Service Now organizations and devices in Service Now. Service Now is directly 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 a 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. An end customer can be connected to only one Service Now partner.

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

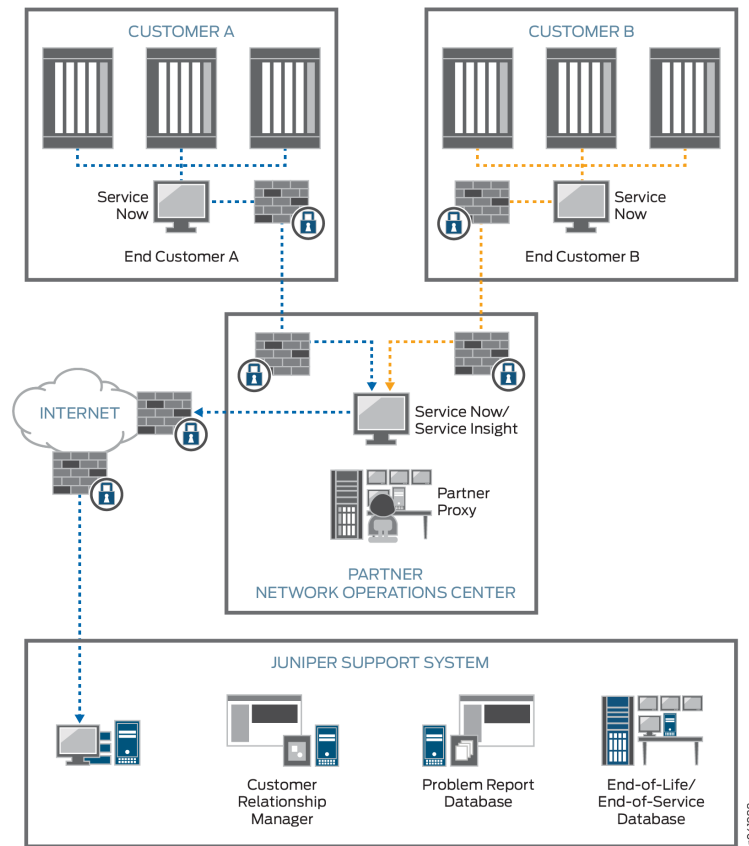


Table 3 on page 22 highlights some of the differences among the various modes of operating Service Now.

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

- [Service Now Administration Workspace 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 the SNMP server you configure on Service Now. The traps correspond to the trigger defined for notification

policies. For information about notification policies, see [“Service Now Notification Policies Overview” on page 135](#).

Using Service Now notifications, you can configure Service Now to send SNMP traps to one or more configured 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 the MIB files:

1. From the list to select Junos Space applications on the Junos Space GUI, select **Service Now**.

The dashboard appears, which displays the **Service Now Notices** box.

2. 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 page provides links to the Service Now MIBs for different Service Now releases.

3. Click a Service Now version to download the respective MIB file.

Related Documentation

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

Service Now Domain Overview

A domain is a logical grouping of objects in Junos Space. A Junos Space administrator creates and manages domains in the Junos Space Network Management Platform. For 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 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 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 in the system domain and objects such as organization, script bundle, SNMP configuration, and Email template, which are assigned to the domain that you are currently in, are visible to you. If you are assigned to more than one domain, you can access the other domains and objects in those domains by selecting the domains from the **Login as username in** list present on the Service Now banner. 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 end customer.

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 • Auto Submit Filter • Incident Filter 	Domain to which a user is logged in	Global 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"> • Global Setting • Directive File • SNMP Configuration • Core File Upload Configuration • Message • Script Bundle • Email Template • End Customer Information Message • Script Installation Advisor (SIA) 	System domain	System domain
<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 page appears.

2. On the Object's 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 to which you want to assign the object 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 on the service Now banner, 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](#)
- *Service Now Administration Workspace 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 28](#) 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
	Incident Filter	All columns except: <ul style="list-style-type: none"> • Attributes
	Auto Submit Filter	All columns except: <ul style="list-style-type: none"> • Attributes
	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
	Suppressed Events	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. Dashboard is the default page that appears on the Service Now GUI when you access the Service Now application.

The Service Now dashboard includes:

- [Service Now Workspaces on page 30](#)
- [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 of Junos Space Network Management Platform by including them in the Service Now navigation tree.

For more details about devices and jobs workspace, refer to [Workspaces Feature Guide](#).

You can perform the following tasks by using the Service Central workspaces:

- View and manage incidents
- View and manage technical support cases
- (only in Partner Proxy mode) View and manage end-customer cases
- View and manage informative messages from Juniper Support System (JSS) or Service Now partner (in End Customer mode)
- View and manage device snapshots
- View and manage BIOS validations and product health data
- View and manage JMB with errors
- View and manage JMBs for which incidents are not created
- Configure and manage notification policies for informing users about events that occurred on devices.

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:

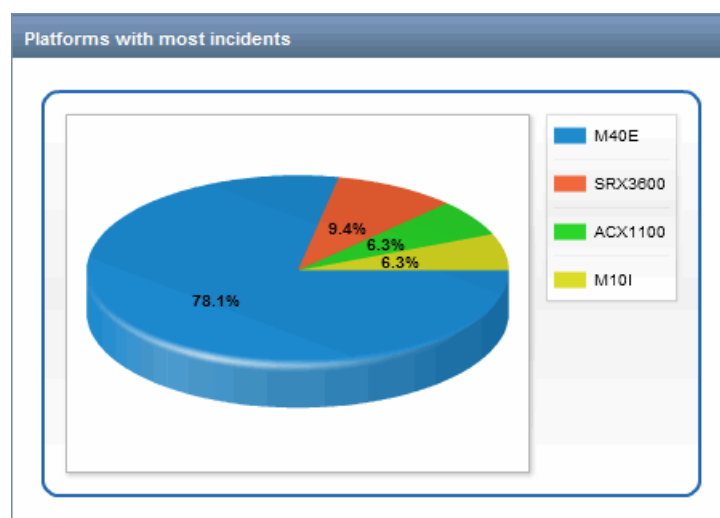
- [Platforms with Most Incidents on page 31](#)
- [Devices with the Most Incidents on page 31](#)
- [Service Now Notices \(Upgrade and Contract Notice\) on page 32](#)

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



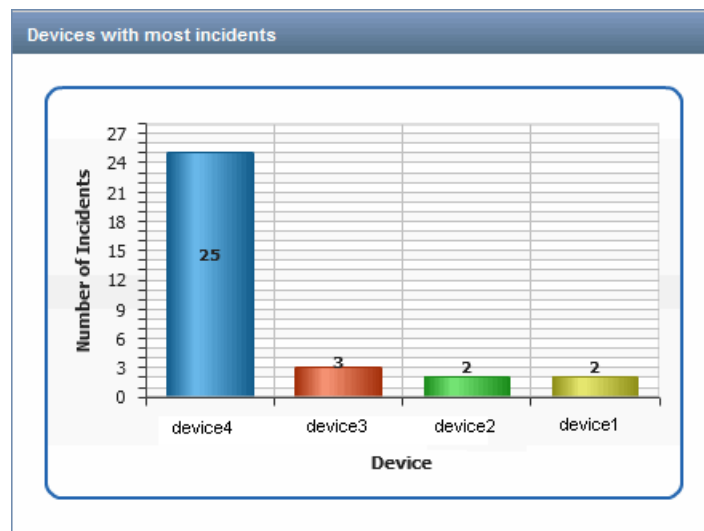
Devices with the Most Incidents

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.

By using the Devices with Most Incidents gadget, you can also filter all incidents created for a device on the Incidents page. To do this, click the **Devices** bar of your choice in the graph to take you to the 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](#)
 - [Service Now Administration Workspace Overview](#)

Service Central Overview

The Service Central workspace of the Service Now application lets you to manage incidents, information messages, device snapshots, notifications, and error JMBs. 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. In response to the JMB received, Service Now creates a new incident for the JMB and displays it on the Incidents page.

The Service Central workspace displays the following three gadgets on its dashboard to display information about incidents graphically:

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

When you click a bar on the graph, service Now takes you to the Incidents page listing only the incidents represented by the bar..

Figure 5: Service Central Gadgets



After viewing an incident, you can submit a case to the Juniper Support Systems (JSS) or a Service Now partner (in End Customer mode). 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.

Service Now considers a JMB 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 you can view or download them for analysis.

Service Now provides the notifications task in Service Central workspace to configure notification policies which define the conditions such as new incident is detected or a new incident is submitted, when service Now must send notifications to users. Notification policies also provide filters that you can use to fine tune the conditions under which you receive a notification.

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* in the [Junos Space Service Now Administration Guide](#).

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:

- **Manage incidents**—You can view, delete, export, submit to create a case, view JMB associated with the incident, and upload core files for the incidents.
- **Manage cases**—You can view the technical support cases that were created for incidents you submitted, collect additional information for the cases, update case with additional notes, and upload attachments for the case.

If Service Now is operating in the Partner Proxy mode, you can view and manage cases for your end customers (also known as connected members).

- **Manage messages and notifications from JSS**—You can view and assign or flag informational messages that you receive from JSS or Service Now partner to specific users.
- **Manage device snapshots (also known as informational JMBs or iJMBs)**—You can view, export the JMB information to an HTML file and delete the iJMBs.
- **View and export BIOS validation data collected from devices**
- **View and export product health data collected from devices**
- **View and download erroneous JMBs**
- **View JMBs for which Service Now did not create incidents**
- **Manage notifications**—You can create, enable or disable and copy notifications information about devices that are susceptible to known issues.

**Related
Documentation**

- [Junos Space Service Now Overview on page 17](#)
- [Service Now Modes](#)
- [Service Now Incidents Overview on page 37](#)
- [Service Now Device Snapshots Overview on page 99](#)
- [Service Now Messages Overview on page 93](#)
- [JMBs with Errors on page 127](#)
- [Service Now Notification Policies Overview on page 135](#)
- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 63](#)
- [Service Now Suppressed Events Overview on page 131](#)

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 section in the Junos Space help that guides you through the tasks that you can perform as part of the initial setup for every Junos Space 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 Junos Space 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 Service Now in Direct mode.

The Getting Started Assistant provides the following steps to start working with Service Now:

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 [Workspaces Feature 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*.

**Related
Documentation**

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

CHAPTER 3

Managing Incidents

- [Service Now Incidents Overview on page 37](#)
- [Viewing Incident Details on page 41](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Flagging an Incident to a User on page 51](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Updating an End-Customer Case on page 54](#)
- [Uploading an Attachment to an Incident on page 55](#)
- [Uploading Core Files to JSS for an Incident on page 57](#)
- [Checking Incident Status Updates on page 58](#)
- [Deleting an Incident on page 59](#)
- [Associating an Incident with an Existing Case on page 59](#)

Service Now Incidents Overview

Junos Space Service Now generates an incident and lists it on the Incidents page (at **Service Central > Incidents**) when a Juniper Message Bundle (JMB) is received. 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 JMB 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. Service Now displays the incidents created on the Incidents page chronologically, by organization

name, and by device group. 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. For information about notifications, see [“Service Now Notification Policies Overview” on page 135](#).

[Table 6 on page 38](#) lists the fields on the Incidents page.

Table 6: 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
Connected Member	
Priority	<p>The priority of the incident</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 1-Critical • 2-High • 3-Medium • 4-Low
Type	The type of defect
Problem Identifier	The ID of the incident
Remarks	Remarks, If any, about errors while reading the JMB, creating the incident, or uploading the incident to Juniper Support Systems (JSS).
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 to which the device belongs
Occurred	The date and time the incident was created on Service Now
Total Core Files	The number of core files available for the incident

Table 6: Fields on the Incidents Page (continued)

Fields	Description
Status	<p>The status of the incident</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Not Submitted—Incident is not submitted to JSS. • Submitted—Incident is submitted to JSS. • Created—A case is created for the incident and an ID is assigned to the case in JSS. • Updated—The case ID of the incident is updated in JSS. • Create Failed—A case could not be created in JSS for the incident. • Closed—The case is closed in JSS. • Submission Failed—The incident could not be submitted to JSS for creating a case. • Associated to a Case—The incident is associated with a case.
Flagged	<p>Specifies whether the incident is lagged to you.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Yes—The incident is flagged to you. • No—The incident is not flagged to you..
Entity	<p>The entity of the device for which the incident was created; for example, Routing Engine (re0, re1), power supply, and FPCs</p>



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).

Associated Actions

You can perform the following actions related to incidents:

- Export JMB to HTML; see [“Exporting a Juniper Message Bundle \(JMB\) to an HTML file” on page 52](#) for details.
- Delete an incident; see [“Deleting an Incident” on page 59](#) 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 43](#) for details.
- View a case in the Juniper Networks Case Manager; see [“Viewing a Case in Case Manager” on page 67](#) for details.
- Assign an incident to a user; see [“Assigning an Owner to an Incident” on page 44](#) for details.
- Flag an incident to a user; see [“Flagging an Incident to a User” on page 51](#) for details.

- Submit an incident to create a JTAC case; see [“Submitting an Incident to Juniper Support Systems or Service Now Partner” on page 45](#) for details.
- Export the summary of an incident to Excel; see [“Exporting Incident Summary to Excel” on page 46](#) for details.
- Update an end customer case; see [“Updating an End-Customer Case” on page 54](#) for details.
- Create auto submit policy for an incident; see [“Creating an Auto Submit Policy” on page 54](#) for details.
- Upload core files to JSS for incidents; see [“Uploading Core Files to JSS for an Incident” on page 57](#) for details.
- Upload attachments; see [“Uploading an Attachment to an Incident” on page 55](#) for details.
- Associate an incident with a case; see [“Associating an Incident with an Existing Case” on page 59](#) for details.



NOTE: From Service Now Release 17.1R1, you can associate an incident with a case which is in the open state.

- Configure Junos OS commands for collecting additional information for an incident; see [“Collecting Additional Information for Service Now Incidents and Cases Overview” on page 74](#) for details.



NOTE: From Service Now Release 17.1R1, you can configure Junos OS commands for collecting information, in addition to the information provided by a JMB, for an incident.

Release History Table

Release	Description
17.1R1	From Service Now Release 17.1R1, you can associate an incident with a case which is in the open state.
17.1R1	From Service Now Release 17.1R1, you can configure Junos OS commands for collecting information, in addition to the information provided by a JMB, for an incident.

Related Documentation

- [Service Now Auto Submit Policy Overview](#)
- [Service Now Devices Overview](#)
- [Service Now Notification Policies Overview on page 135](#)

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.
- Collect Additional Information Attachment Details tab: Provides details about the information collected for an incident in addition to information provided by JMBs. The additional information is collected by executing Junos OS commands on devices by a user.



NOTE: Starting Service Now Release 17.1R1, the Collect Additional Information Attachment Details tab is displayed on the Incident Detail page to provide details about the information collected in addition to information provided by JMBs.

To view details of an incident:

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 Incident 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, Log File Details, and Collect Additional Information Attachment Details tab as shown in [Figure 6 on page 42](#). 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' window with the following tabs: Incident Details (selected), Case Details, Core File Details, Attachment Details, Log File Details, and Collect Additional Information Attachment Details. The main content area displays the following information:

- Device: sn-space-ex4550-sys
- IP Address: 10.219.30.157
- Device Serial Number: LX0213163855
- Product: EX4550-32F
- Platform: junos-ex
- Release: 15.1R5.5
- Organization: Prod_Org
- Device Group: Default for TestORG
- Connected Member:
- Occurred: May 26, 2017 1:48:45 PM IST
- Status: Case Associated, 2017-0526-0673
- Problem Identifier: sn-space-ex4550-sys-279-20170526-081843-279
- Event Type: Software Failure
- Defect Type: File system error
- Entity: re0
- Job Id: ---
- Filter Name:
- KB Article: <http://kb.juniper.net/InfoCenter/index?page=content&actp=SN&id=KB18770>

An 'OK' button is located at the bottom right of the window.

You can retrieve required information from the tabs.

Release History Table

Release	Description
17.1R1	Starting Service Now Release 17.1R1, the Collect Additional Information Attachment Details tab is displayed on the Incident Detail page to provide details about the information collected in addition to information provided by JMBs.

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Deleting an Incident on page 59](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 54](#)
- [Troubleshooting Issues with Creating Incidents](#)
- [Associating an Incident with an Existing Case on page 59](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)

Viewing Knowledge Base Articles Associated with an Incident

A Knowledge Base (KB) article provides information about the causes and solutions for a problem. Junos Space Service Now provides the View KB Article in the Actions list to 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 for which you want to view the KB article 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 KB articles.

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Deleting an Incident on page 59](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)
- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 54](#)

Assigning an Owner to an Incident

Junos Space Service Now provides the Assign Ownership option on the Actions list of the Incidents page to assign a user to look into the 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 web-based dialog box titled "Assign Ownership" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Enter the Login ID of User" with a text input field containing the word "super" and a search icon (magnifying glass) to its right. Below this, there is a checked checkbox followed by the text "Email Incident to Assigned Owner". At the bottom of the dialog, there are two buttons: "Submit" and "Cancel".

3. Enter the login ID of the Service Now 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**.

Service Now assigns the incident to the specified user. .

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Flagging an Incident to a User on page 51](#)
- [Deleting an Incident on page 59](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)
- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 54](#)

Submitting an Incident to Juniper Support Systems or Service Now Partner

Junos Space Service Now provides the Submit Case option in the Actions list of the incidents page to submit an incident to Juniper Support Systems (JSS) or Service Now partner (in End Customer mode) for creating a case. After you submit an incident, Service Now changes the incident status to Submitted. For Service Now operating in the End Customer mode, the incident is submitted to the Service Now partner. The Service Now partner can submit the incident from the end customer to JSS.

If you have an auto submit policy configured to submit an incident for opening a case, Service Now submits the incident immediately after the incident is created. Starting with Service Now Release 17.2R1, Service Now provides the option *Minimum Incident Submission Delay Time (In Mins)* for configuring the time after which the incident should be submitted for creating a case. By configuring a time to delay submitting an incident, you can choose not to submit the incident until the time delay.



NOTE: Service Now displays the Submitted status in red if an error or exception has occurred while submitting the incident to JSS or Service Now partner. 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:

- *Event* indicates the incident was generated due to an event in a device.
- *On Demand* indicates on-demand incidents generated by Service Now
- *Event RMA* indicates RMA incidents detected by AI-Scripts
- *Event (low end)* indicates
- *On Demand RMA* indicates 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. Service Now automatically uploads the JMB attachments to the related case after collecting them from the device.

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 list, select **Submit Case**. Alternatively, right-click the incident and select **Submit Case**.

Figure 7 on page 47 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.



NOTE: Site ID and User Name can be modified only if Service Now is operating in the Direct or Partner Proxy mode. In End Customer mode, Site ID and Username fields are not visible on the Submit Case Options page.

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

- c. (Optional) Select the **Save As Default User For Incident Submission** check box if you want to submit incidents for that site only for the selected user .
 - For a new user:
 - a. Click **User Name**.
 - b. 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.
 - c. In the **Password** field, enter the password to log in to the organization.
The password is provided by Juniper Networks.
 - d. Click the **Get Sites** link.
The Site ID list displays a list of site IDs associated with the user name.
 - e. 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 Direct, 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. If needed, you can create a new address group and associate it with the device or you can select any other configured address group for creating a case.
- For an end-customer device, in the Partner Proxy mode, the Address Group and Ship-to Address fields are prepopulated with the address group sent by the end-customer and the address group present in the system for opening a case. The Service Now partner has the option of changing this value to an address group present in their system.
- If the Service Now 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 address provided by the end-customer.
- If a device is not associated with an address group, None is displayed in the Address Group field for that device.

The address group selected on the Submit Case page is submitted as the shipping address to the Service Now partner.

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 text or 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 mode.

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) In the **Minimum Incident Submission Delay Time (In Mins)** field enter the number of minutes by which you want Service Now to delay submitting the incident for creating a case.

You can delay submitting an incident by 1 – 21600 minutes.

14. (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.

15. (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

16. Select one or more core files to upload.

The core files are uploaded after the case is created for the incident.

17. (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.

18. (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.

19. Select the device components for which you want to request RMA incidents and click **Submit**.

20. In the **Problem Description** field, enter information about the device components (part number, version, part description, part serial number, and so on).

21. 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.

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

The Incidents page appears.

23. 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.

24. 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.

25. 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

- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Viewing Incident Details on page 41](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 54](#)

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 page 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**.

Service Now sends an e-mail notification for the incident to all the selected users.

**Related
Documentation**

- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Deleting an Incident on page 59](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)
- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 54](#)

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

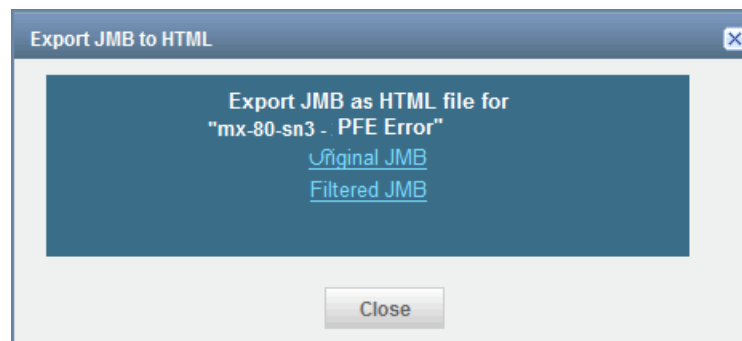
Junos Space Service Now provides the Export JMB to HTML option in the Actions list to export JMB data along with its attachments as HTML files and save them on your local file system. A JMB is exported as a zipped folder. Logs are not exported. The view of the exported JMB file is the same as of the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

To export a JMB 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 for which you want to export JMB
3. From the Actions list, 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 53](#).

Figure 8: Export JMB to HTML Dialog Box



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

5. The browser opens the dialog box to save or open the JMB file.

Click **Save** to save the JMB as an HTML file or **Open** to open the JMB file.

To export an incident data as an Excel file:

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.

3. 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.

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

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Deleting an Incident on page 59](#)
- [Checking Incident Status Updates on page 58](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)

- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 54](#)

Updating an End-Customer Case

In Partner Proxy mode, Junos Space Service Now provides the End Customer Cases option to submit an end-customer incident to create a case



NOTE: This action is enabled only when the status of the end-customer 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 54](#).

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 and 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](#)
- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Deleting an Incident on page 59](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)
- [Viewing a Case in Case Manager on page 67](#)

Uploading an Attachment to an Incident

Junos Space Service Now provides the Upload Attachment option on the Actions list 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.

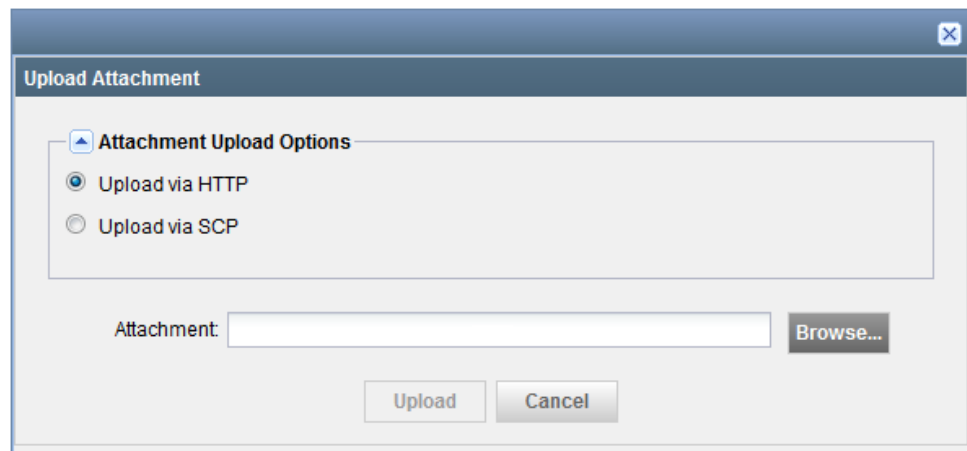
The attachment is stored in Service Now if the incident is not submitted to JSS. If a case is already created for the incident, the attachment, when uploaded to the incident is automatically uploaded to the case as well. An attachment that is uploaded to Service Now can be viewed on the View JMB page 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 list, 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, select an option to upload an attachment as follows:

- 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**.

Service Now initiates the upload of the attachment and displays the File Upload Job information dialog box.

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

Related Documentation

- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 63](#)
- [Service Now Incidents Overview on page 37](#)
- [Uploading an Attachment to a Case on page 70](#)

Uploading Core Files to JSS for an Incident

Junos Space Service Now provides the Upload Core Files option in the Actions list to upload core files generated for an event to Juniper Support Systems (JSS) or Service Now Partner. This option is enabled only when there is at least one core file available for upload.

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

When an end customer uploads core files, the core files are uploaded to the SFTP server configured by the Service Now partner. The Service Now partner provides the ID of the case for the incident submitted by the end customer. The case ID provided by the Service Now partner can be an ID created internally by the Service Now partner or created by JSS. In either case, the core files are uploaded automatically to the SFTP server once a case is created.

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**
- [Service Now Incidents Overview on page 37](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
 - [Configuring SFTP Server for Uploading Core Files Generated for Events](#)
 - [Updating Core File Upload Configuration for an End Customer](#)

Checking Incident Status Updates

You can use the Incidents page to submit an incident to JSS or Service Now partner 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 the following 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 137](#).
- 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 you last logged in.

To view the graphs on the Service Central page, click **Service Central** from the Service Now navigation tree.

- Related Documentation**
- [Service Now Incidents Overview on page 37](#)
 - [Assigning an Owner to an Incident on page 44](#)
 - [Flagging an Incident to a User on page 51](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
 - [Deleting an Incident on page 59](#)
 - [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
 - [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
 - [Viewing Incident Details on page 41](#)
 - [Viewing a Case in Case Manager on page 67](#)
 - [Updating an End-Customer Case on page 54](#)
 - [Associating an Incident with an Existing Case on page 59](#)

Deleting an Incident

Junos Space Service Now provides the Delete action in the Actions list of the Incidents page to delete incidents.

Service Now provides the Submitted Incident Purge Time and Not Submitted Incident Purge Time parameters in global settings to configure the number of days after which incidents that are submitted or incidents that are not submitted can be deleted automatically from the Service Now database. The Delete option provides you the flexibility to delete incidents whenever you want to delete before the configured purge time.

To delete incidents:

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

The Incidents table appears.

2. Select one or more incidents that you want to delete.

3. Click **Delete**.

The selected incidents are removed from the Incidents table and the Service Now database.

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 43](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)
- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 54](#)

Associating an Incident with an Existing Case

Starting Junos Space Service Now Release 17.1R1, you can associate a new incident with technical support cases that are not closed. When you associate an incident with a case, the status of the incident on the Incidents page is set to **Case Associated** along with the **ID** of the case with which the incident is associated. You can also view the ID of the case with which the incident is associated on the Case Details tab of the Incident Details page.

The attachments and log files of the incident are uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode) and associated with the related case.



NOTE:

- To associate an incident with a case, the case should not be in the Closed state.
- An incident created for a BIOS JMB cannot be associated with a case.
- Once an incident is associated with a case, the association cannot be undone.
- An incident in one domain can be associated with a case assigned to another domain. A case can be associated with multiple domains.
- When an incident (I1) is associated with a case that is created by submitting another incident (I2), the incident I1 is deleted or purged when incident I2 is deleted or purged.

To associate a new incident with an existing case:

1. In the Service Now navigation tree, click **Service Central > Incidents**.

The Incidents page appears.

2. Select an incident that you want to associate with an existing case.

3. Select **Associate Case** from the Actions list or the right-click menu.

The Associate Case ID page appears as shown in [Figure 11 on page 60](#).

Figure 11: Associate Case ID Page

Associate Case Id

Case Id: 2017-0721-0002

Incident Information:

Event Incident details associated with the case:

Hostname - mx-480-sn

Incident Occurred date - 24 Nov 2017 06:33:25 GMT Etc/UTC

Event type - Software Failure

Defect type - File system error

Problem Identifier - mx-480-sn-279-20171123-223324-279

Problem Synopsis - AV_PATTERN_TOO_BIG

Customer Comment:

Sample Association

Submit Cancel

4. In the **Case Id** text field, enter the Case ID with which you want to associate the incident.



NOTE: To associate an incident with a case, the case should be listed in the Technical Support Cases page and the status should not be Closed.

5. (Optional) Enter a comment when you associate the selected incidents with the case in the **Customer Comment** text field.

The incident information together with the customer comment appear as case notes (incident information listed first followed by the customer comment) in Case Manager. Total number of characters allowed in a case note is (incident information and customer comment) is 39000.

6. Click **Submit** to associate the selected incidents with the case.

Service Now associates the incidents with the case and sends the incident information and customer comments to Case Manager as case notes.

You can verify whether or not the incident is associated with a case by checking the status of the incident on the Incidents page (Service Central > Incidents). The status of the incident should be **Case Associated** along with the **case ID**.

Release History Table

Release	Description
17.1R1	Starting Junos Space Service Now Release 17.1R1, you can associate a new incident with technical support cases that are not closed.

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 63](#)
- [Viewing Incident Details on page 41](#)
- [Checking Incident Status Updates on page 58](#)

CHAPTER 4

Managing Cases

- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 63](#)
- [Viewing a Case in Case Manager on page 67](#)
- [Updating an End-Customer Case on page 68](#)
- [Uploading an Attachment to a Case on page 70](#)

Service Now Technical Support Cases 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 Systems (JSS) and a case ID is assigned to the incidents. You can view the technical support cases on the View Tech Support page (**Service Central > Tech Support Case**) of the Service Central workspace.



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

Starting in Service Now Release 15.1R1, the Site ID and Device Name columns are provided on the View Tech Support Cases page when Service Now is operating in Partner Proxy and Direct modes to allow filtering cases based on site ID and device name. On the View End Customer Cases page, the Device Name column is provided to filter end-customer cases based on device name.

[Figure 12 on page 64](#) shows the View Technical Support Cases page.

Figure 12: View Tech Support Cases

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

Starting in Service Now Release 16.1R1, the Case Details page of a Service Now partner displays case notes for the Service Now partner and End Customer Service Now on different tabs.

Table 7 on page 64 lists the columns displayed on the View Tech Support Cases page:

Table 7: 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 the 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

Table 7: Fields on the View Tech Support Cases Page (continued)

Field	Description
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
Priority	<p>Priority of the case.</p> <p>Possible values are:</p> <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 (**Service Central > View End Customer Cases**) of the Service Central workspace. The Service Now partner updates the status of the case to the Service Now end customer.

Figure 13 on page 65 shows the View End Customer Cases page.

Figure 13: View End Customer Cases Page

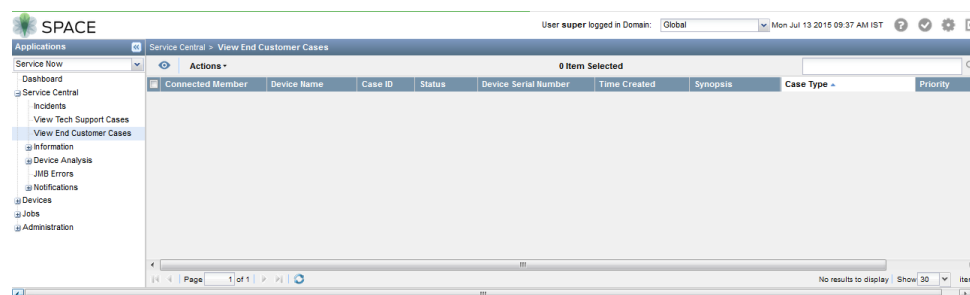


Table 8 on page 66 lists the columns displayed on the View End Customer Cases page:

Table 8: 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
Priority	<p>Priority assigned to the incident, by the end customer, for whom the case is created</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • 1 - Critical • 2- High • 3 - Medium • 4 - Low

Associated Actions

You can perform the following tasks related to tech support and end-customer cases:

- View details of a technical support case in Case Manager; see [“Viewing a Case in Case Manager” on page 67](#) for details.
- Add notes to a technical support case; see *Adding Notes to a Technical Support Case* for details.

- Upload binary or text attachments for a technical support case; see [“Uploading an Attachment to a Case” on page 70](#) for details.
- Configure Junos OS commands for collecting additional information for a case; see [“Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case” on page 85](#) for details.
- Update an end-customer support case; [“Updating an End-Customer Case” on page 54](#) for details.
- View details of an end-customer case in Case Manager; see [“Viewing a Case in Case Manager” on page 67](#) for details.

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16.1R1, the Case Details page of a Service Now partner displays case notes for the Service Now partner and End Customer Service Now on different tabs.
15.1R1	Starting in Service Now Release 15.1R1, the Site ID and Device Name columns are provided on the View Tech Support Cases page when Service Now is operating in Partner Proxy and Direct modes to allow filtering cases based on site ID and device name. On the View End Customer Cases page, the Device Name column is provided to filter end-customer cases based on device name.

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Service Now Notification Policies Overview on page 135](#)
- [Service Now Organizations Overview](#)
- [Junos Space Service Now Global Settings Overview](#)

Viewing a Case in Case Manager

You can view the details of a case submitted to JSS or Service Now partner 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 for a user ID and password at <https://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.

You can view a case in Case Manager by using Service Now in the following two ways—By using the Incidents task or by using the View Tech Support Case or View End Customer Case task

To view a case in Case Manager:

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

The Incidents page appears.

Alternatively, you can also select **Service Central > View Tech Support Cases..**

The View Tech Support Cases page appears.

In a Service Now operating in Partner Proxy mode, if you want to view an end-customer case in Case Manager, select **Service Central > View End Support Cases.**

The View End Customer Cases page appears.

2. On the Incidents page, select the incident for which you want to view details of the associated case in the Case Manager, and select **View Case in Case Manager** from either the **Actions** list or the right-click menu.



NOTE: If the **View Case in Case Manager** link is not enabled on the Incidents page, verify whether a case is created for the incident.

On the View Tech Support Cases or View End Customer Cases page, select the case that you want to view in 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.

3. Enter your username and password and click **Login**.

The JSS Case Manager displays the case details.

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Deleting an Incident on page 59](#)
- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)
- [Updating an End-Customer Case on page 54](#)

Updating an End-Customer Case

In Partner Proxy mode, Junos Space Service Now provides the End Customer Cases option to submit an end-customer incident to create a case



NOTE: This action is enabled only when the status of the end-customer 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 54](#).

Figure 14: End-Customer Cases Dialog Box

The screenshot shows a dialog box titled "End Customer Cases" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Case ID:** ECC1
- Case Link:** An empty text input field.
- Case Status:** A dropdown menu currently showing "Updated".
- 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

At the bottom of the dialog are two buttons: "Submit" and "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](#)
- [Service Now Incidents Overview on page 37](#)
- [Assigning an Owner to an Incident on page 44](#)
- [Flagging an Incident to a User on page 51](#)
- [Deleting an Incident on page 59](#)

- [Checking Incident Status Updates on page 58](#)
- [Exporting a Juniper Message Bundle \(JMB\) to an HTML file on page 52](#)
- [Submitting an Incident to Juniper Support Systems or Service Now Partner on page 45](#)
- [Viewing Incident Details on page 41](#)
- [Viewing a Case in Case Manager on page 67](#)

Uploading an Attachment to a Case

Service Now provides the Upload Attachment option in the Actions list to upload a file, for example, a text, image, or binary file, as an attachment to a case created in Juniper Support Systems (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. However, attachments uploaded by an end customer are stored in Service Now partner.



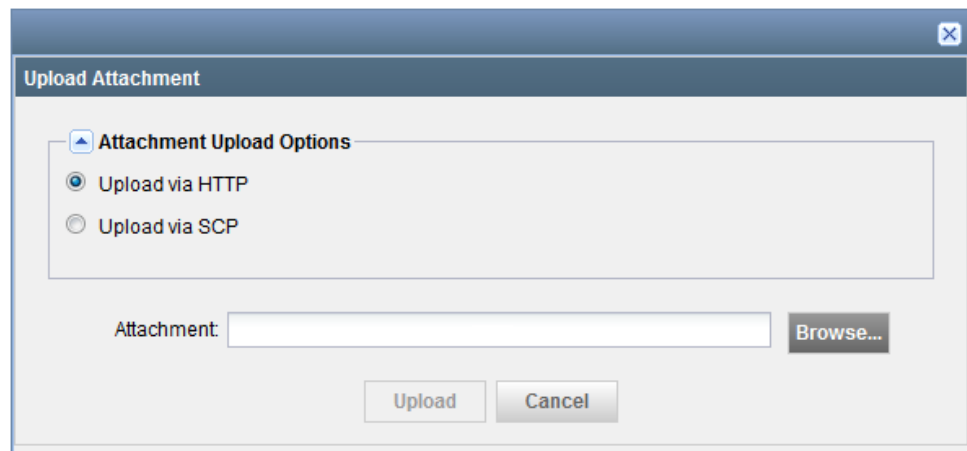
NOTE: We recommend that you limit the size of an attachment to be uploaded to 1 GB and use Secure Copy Protocol (SCP) to upload files of size 1 GB.

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 list, select **Upload Attachments**. Alternatively, right-click the case and select **Upload Attachments**.

The Upload Attachment dialog box appears as shown in [Figure 15 on page 71](#).

Figure 15: 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 from which you want to upload the attachment.
 - **Software File Path:** Specify the file path to access the Service Now image file on the local machine.
- c. Click **Submit**.

Service Now starts uploading the attachment and the File Upload Job dialog box displays the progress of the upload job. Close the dialog box after the job is complete.

- Related Documentation**
- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 63](#)
 - [Service Now Incidents Overview on page 37](#)
 - [Uploading an Attachment to an Incident on page 55](#)

CHAPTER 5

Collecting Additional Information for Incidents and Cases

- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)
- [Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident on page 78](#)
- [Modifying the Settings for Collecting Additional Information for an Incident on page 79](#)
- [Deleting the Settings for Collecting Additional Information for an Incident on page 81](#)
- [Downloading the Additional Information Collected About an Incident on page 82](#)
- [Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case on page 84](#)
- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 85](#)
- [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 88](#)
- [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 90](#)
- [Downloading the Additional Information Collected for a Technical Support Case on page 91](#)

Collecting Additional Information for Service Now Incidents and Cases Overview

Starting in Junos Space Service Now Release 17.1R1, for an incident (**Service Central > Incidents**) or a technical support case (**Service Central > View Technical Support Case**), you can collect information in addition to what is available in a Juniper Message Bundle (JMB) by executing Junos OS commands on the device for which the incident and case are created. The additional information can be collected for an incident either before submitting the incident for opening a case or after the case is created. If a case is already created for the incident, the additional information collected can be directly uploaded to Juniper Support Systems (JSS) and associated with the case.

You can define the commands that can be executed to collect the additional information and the intervals at which the commands should be executed.

The additional information is collected from the device as a text file with the name **additional_cli_information_<devicename>_<timestamp>.txt** and associated with the incident in the Service Now database or uploaded to JSS if a technical support case is already created for the incident. If you are collecting additional information for a case, Service Now uploads the information directly to JSS from the device. For Service Now operating in the End Customer mode, the additional information is uploaded to the Service Now partner from where it is uploaded to JSS, if required.



NOTE:

- A Service Now partner cannot configure commands for collecting additional information for incidents or cases for its end customers.
 - Additional information cannot be collected for incidents and cases that are in the closed state.
-

Associated Actions

You can perform the following actions related to collecting additional information for an incident or case:

- Configure Junos OS commands to collect information for an incident; see [“Configuring Junos OS Commands to Collect Additional Information About an Incident”](#) on page 75 for details.
- View Junos OS commands configured to collect information; see [“Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident”](#) on page 78 for details.
- Modify Junos OS commands configured to collect information for an incident; see [“Modifying the Settings for Collecting Additional Information for an Incident”](#) on page 79 for details.
- Delete Junos OS commands configured for collecting information for a case; see [“Deleting the Settings for Collecting Additional Information for an Incident”](#) on page 81 for details.

- Download information collected for an incident; see [“Downloading the Additional Information Collected About an Incident” on page 82](#) for details.
- View Junos OS commands configured for collecting additional information for a technical support case; see [“Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case” on page 84](#) for details.
- Configure Junos OS commands configured for collecting additional information for a technical support case; see [“Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case” on page 85](#) for details.
- Modify Junos OS commands configured for collecting additional information for a technical support case; see [“Modifying the Configuration for Collecting Additional Information for a Technical Support Case” on page 88](#) for details.
- Delete Junos OS commands configured for collecting additional information for a technical support case; see [“Deleting the Configuration for Collecting Additional Information for a Technical Support Case” on page 90](#) for details.
- Download Junos OS commands configured for collecting additional information for a technical support case; see [“Downloading the Additional Information Collected for a Technical Support Case” on page 91](#) for details.

Release History Table

Release	Description
17.1R1	Starting in Junos Space Service Now Release 17.1R1, for an incident (Service Central > Incidents) or a technical support case (Service Central > View Technical Support Case), you can collect information in addition to what is available in a Juniper Message Bundle (JMB) by executing Junos OS commands on the device for which the incident and case are created.

Related Documentation

- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 63](#)
- [Service Now Incidents Overview on page 37](#)

Configuring Junos OS Commands to Collect Additional Information About an Incident

From Junos Space Service Now Release 17.1R1, in addition to the information provided by a JMB for an incident, you can configure Junos OS commands on the Incidents page for collecting additional information about the incident. When you configure commands to collect additional information, the commands you entered are executed on the device and the output is saved in a *.txt file and uploaded to the Service Now database. If a case is already created for the incident, the file is directly uploaded to Juniper Support Systems (JSS) or a Service Now partner (in case of End Customer mode).



NOTE:

- A Service Now partner cannot configure commands for collecting additional information about incidents or cases for its end customers.
- You cannot configure commands for collecting additional information for BIOS incidents and incidents that are closed.

To collect additional information about an incident by executing Junos OS commands:

1. From the Service Now Navigation tree, select **Service Central > Incidents**.
The Incidents page appears.
2. Select the incident about which you want to collect additional information.
3. Select **Collect Additional Information > Create** from the Actions list or the right-click menu.

The Collect Additional Information page appears as shown in [Figure 16 on page 76](#).

Figure 16: Collect Additional Information Page

Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: Multiple commands should be entered as , or ; or new line character.

☒ **Schedule at a later time**
 Start: 05/21/17 6:25 PM IST

☒ **Repeat**
 Interval: Weekly Every 1 Weeks
☒ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

Ends on: ☒ Never 05/21/17 6:25 PM IST

Submit Cancel

4. In the CLI Commands text box, enter the commands for collecting additional information



NOTE: Service Now does not validate the commands that you enter for collecting additional information. To add multiple commands, use comma (,) or semi-colon (;) or the new line character (press Enter on keyboard) consistently as the delimiter.

5. (Optional) Select the **Schedule at a later time** check box and select the date and time when you want the commands to be executed.



NOTE: Service Now executes the commands immediately if you do not schedule a date and time for the commands to be executed.

6. (Optional) Select the **Repeat** check box and select the time interval and the frequency of executing the commands.

You can select the intervals in minutes, hours, daily, weekly, monthly, or yearly to collect additional information. By default, an interval of once a week is selected.

7. (Optional) To define an end time for collecting information for the incident, do one of the following task:

- Click **Never** to continue collecting information by executing the commands at the defined interval until the incident is closed. This option is selected by default.
- Select the date and time when the commands should stop executing.

8. Click **Submit** to save the configuration or **Cancel** to cancel the configuration.

Service Now collects additional information immediately if the Schedule at a later time check box is not selected.

See ["Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident" on page 78](#) to check whether the job to collect additional information is successful or not.

Release History Table

Release	Description
17.1R1	From Junos Space Service Now Release 17.1R1, in addition to the information provided by a JMB for an incident, you can configure Junos OS commands on the Incidents page for collecting additional information about the incident .

Related Documentation

- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)
- [Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident on page 78](#)

- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 85](#)
- [Deleting the Settings for Collecting Additional Information for an Incident on page 81](#)

Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident

You can view the Junos OS commands that are configured for collecting additional information about an incident on the Collect Additional Information Jobs Results Summary page. The Collect Additional Information Jobs Results Summary page displays the following information:

- Commands that are executed to collect additional information
- Name of the text file in which the command outputs are collected
- Status of the command execution
- Date and time the information was collected or is scheduled to be collected
- Job ID for executing the command
- User who configured the command
- Whether or not commands should be executed recurrently
- Remarks, if any, to indicate any issues that might have occurred while the commands for collecting additional information are executed

[Figure 17 on page 78](#) shows the Collect Additional Information Jobs Results Summary page.

Figure 17: Collect Additional Information Jobs Results Summary page

Collect Additional Information Jobs Result Summary							
Back							
Commands	File Name	Job Status	Scheduled Time	Job Id	Owner	Recurrence	Remarks
<input type="checkbox"/> show version	---	Scheduled	May 21, 2017 6:20:41 PM IST	1348115	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550- sys_20170521-124843926. txt	Success	May 21, 2017 6:18:41 PM IST	1348113	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550- sys_20170521-124643891. txt	Success	May 21, 2017 6:16:41 PM IST	1348111	super	Every 2 minutes First Occurrence: 2017-05-21 12:46:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550- sys_20170521-124444786. txt	Success	May 21, 2017 6:14:41 PM IST	1348109	super	Every 2 minutes First Occurrence: 2017-05-21 12:44:41.434	

To view Junos OS commands that are configured for collecting additional information for an incident:

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

The Incidents page appears.

2. Select the incident for which you want to view the commands configured for collecting additional information.
3. Select **Collect Additional Information > View** from the Actions list or the right-click menu.

The Collect Additional Information Jobs Results Summary page appears. The commands column lists the commands executed for collecting additional information and the Status column indicates whether the commands were executed successfully or not.

Related Documentation

- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)
- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 85](#)

Modifying the Settings for Collecting Additional Information for an Incident

If the job to collect additional information is not already executed, you can modify the following attributes in a configuration for collecting additional information about an incident:

- Junos OS commands configured for collecting additional information
- Date and time the commands should be executed
- interval for executing the commands if the commands are configured to be executed repeatedly

To modify the configuration for collecting additional information for an incident:

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

The Incidents page appears.

2. Select the incident for which you want to modify the settings for collecting additional information.
3. Select **Collect Additional Information > Modify** from the Actions list or the right-click menu.

The Modify Collect Additional Information page appears as shown in [Figure 18 on page 80](#).



NOTE: The Modify option is disabled if the job to collect additional information is in progress or already complete.

Figure 18: Modify Collect Additional Information page

Modify Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: show version

☒ **Schedule at a later time**

Start: 05/21/17 6:28 PM IST

☒ **Repeat**

Interval: Minutes Every 2 Minutes

Ends on: ☒ Never ☐ 05/21/17 6:28 PM IST

Submit **Cancel**

4. (Optional) Modify the commands in the **CLI Commands** text box.
5. (Optional) Modify the schedule for executing the commands under the **Schedule at a later time** section.
6. (Optional) Modify the frequency at which the commands should be executed under the **Repeat** section.
7. Click **Submit**.
 The job to collect information is rescheduled and the job ID is displayed.
8. (Optional) Click the job ID to view the job details.
 The Job Details page displays the progress of the job.

Related Documentation

- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)

- [Viewing Junos OS Commands Configured for Collecting Additional Information About an Incident on page 78](#)
- [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 88](#)

Deleting the Settings for Collecting Additional Information for an Incident

You can delete a non-recurring configuration for collecting additional information that is scheduled to be executed later by deleting the job from the Jobs workspace of the Service Now navigation tree.

A recurring configuration can be deleted by modifying the configuration. When you modify a recurring configuration, the old configuration is deleted and a new configuration is created with the modifications. You can modify a recurring configuration even if it is already executed one or more number of times. If you want to delete the recurring configuration entirely, then the configuration has to be deleted from the Jobs workspace.

To delete a configuration for collecting additional information from the Jobs workspace:

1. On the Service Now navigation tree, click **Jobs > Job Management**.

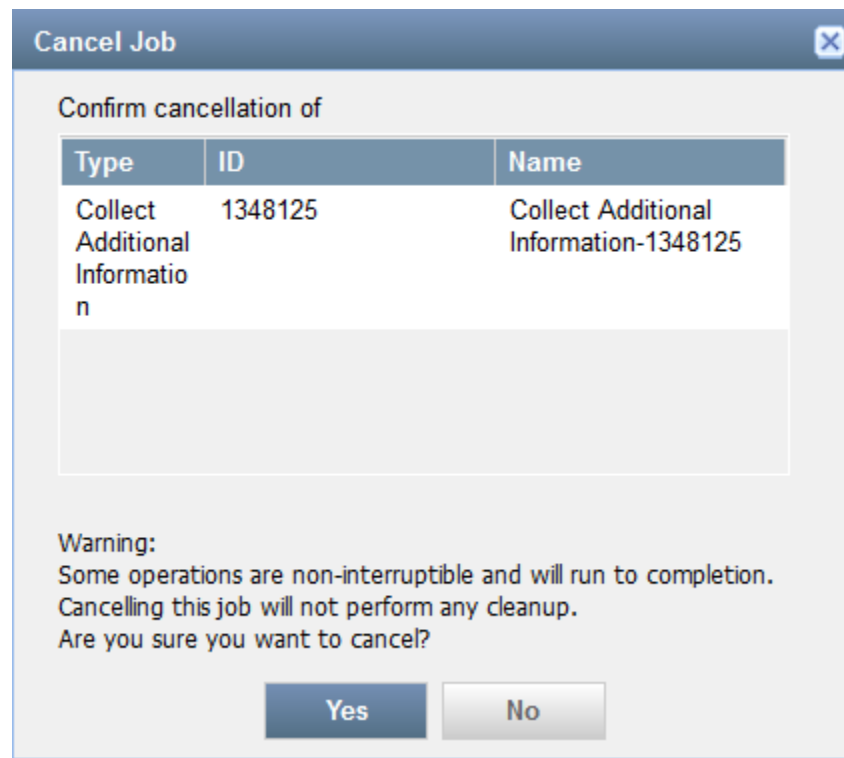
The Job Management page appears.

2. Select the Collect Additional Command job to be deleted.

3. Select **Cancel Job** from the Actions list or the right-click menu.

A confirmation message appears as shown in [Figure 19 on page 82](#).

Figure 19: Cancel Job Dialog Box



4. Click **Yes**.

The job is canceled and the **State** of the job is changed to **Cancelled** from **Scheduled**.

Related Documentation

- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)
- [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 90](#)

Downloading the Additional Information Collected About an Incident

You can download the additional information collected about an incident from the Collect Additional Information Attachment Details tab of the Incident Detail page. The Collect Additional Information Attachment Details tab of the Incident Detail page provides the following information and the **Download all additional information attachments** link to download the attachments:

- Name of the file containing the additional information
- Size of the file (in bytes)

- User who configured the Junos OS commands to be executed for collecting additional information
- Status of reading the additional information collected on a device
- Status of uploading the additional information to JSS or Service Now partner



NOTE: Incidents for which a technical support case does not exist, the upload status is displayed as **Not Uploaded**.

- Remarks, if any, about the additional information collected for the incident

To download the additional information collected for an incident:

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

The Incidents page appears.

2. Double-click the incident for which you want to download additional information collected.

The Incident Detail page appears as shown in [Figure 20 on page 83](#).

Figure 20: Collect Additional Information Attachment Details Tab on the Incident Details Page

Incident Detail					
Incident Details	Case Details	Core File Details	Attachment Details	Log File Details	Collect Additional Information Attachment Details
Download all additional information attachments					
File Name	File Size (in bytes)	Created By	Read Status	Upload Status	Remarks
additional_cli_information_sn-space-ex4550-sys_20170518-113839193.txt	491	super	Success	Success	
additional_cli_information_sn-space-ex4550-sys_20170518-114444902.txt	491	super	Success	Success	
OK					

3. Click the **Collect Additional Information Attachment Details** tab and then click the **Download all additional information attachments** link.

Service Now presents the attachments containing outputs of the additional commands in the *.zip format for download.

4. Download the attachment and save it on your local system.

Related Documentation

- [Downloading the Additional Information Collected for a Technical Support Case on page 91](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)

Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case

You can view the Junos OS commands configured for collecting additional information for a technical support case on the Collect Additional Information Jobs Results Summary page. The Collect Additional Information Jobs Results Summary page displays the following information:

- Commands executed to collect additional information
- Name of the text file in which the command outputs are collected
- Status of executing the command to collect information
- Date and time the information was collected or is scheduled to be collected
- Job ID for executing the command
- User who configured the command
- Whether or not commands should be executed recurrently
- Remarks, if any

[Figure 21 on page 84](#) shows the Collect Additional Information Jobs Results Summary page.

Figure 21: Collect Additional Information Jobs Results Summary Page

Collect Additional Information Jobs Result Summary							
Back							
Commands	File Name	Job Status	Scheduled Time	Job Id	Owner	Recurrence	Remarks
<input type="checkbox"/> show version	---	Scheduled	May 21, 2017 6:20:41 PM IST	1348115	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550-sys_20170521-124843926.txt	Success	May 21, 2017 6:16:41 PM IST	1348113	super	Every 2 minutes First Occurrence: 2017-05-21 12:48:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550-sys_20170521-124643891.txt	Success	May 21, 2017 6:16:41 PM IST	1348111	super	Every 2 minutes First Occurrence: 2017-05-21 12:46:41.434	
<input type="checkbox"/> show version	additional_cli_information_s n-space-ex4550-sys_20170521-124444786.txt	Success	May 21, 2017 6:14:41 PM IST	1348109	super	Every 2 minutes First Occurrence: 2017-05-21 12:44:41.434	

To view the Junos OS commands configured for collecting additional information:

1. From the Service Now Navigation tree, select **Service Central > View Tech Support Cases**.

The View Tech Support Cases page appears.

2. Select the incident for which you want to view the commands that are configured for collecting additional information.
3. Select **Collect Additional Information > View** from the Actions list or the right-click menu.

The Collect Additional Information Jobs Results Summary page appears. The commands column lists the commands executed for collecting additional information and the Status column indicates whether the commands were executed successfully or not.

**Related
Documentation**

- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)
- [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 88](#)
- [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 90](#)
- [Downloading the Additional Information Collected for a Technical Support Case on page 91](#)

Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case

You can configure Junos OS commands to collect additional information for a technical support case on the View Tech Support Cases page. When you configure additional information to be collected, the commands you configured are executed on the device and the output collected in a ***.txt** file and uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode).



NOTE:

- A Service Now partner cannot execute Junos OS commands to collect additional information for end-customer support cases. An end customer has to configure the commands for collecting additional information and upload the additional information to the Service Now partner. The Service Now partner, if required, uploads the additional information to JSS.
 - You cannot collect additional information for cases that are closed and cases related to BIOS incidents.
 - For cases associated with a specific siteID (for example, OSSJ cases or cases created by using Case Manager) that are not generated by incidents submitted by Service Now, the option to collect additional information is disabled on the Tech Support Cases page. However, for incidents that are associated with such cases, the option to collect additional information is enabled on the Incidents page.
 - The Junos OS commands configured for collecting additional information are executed on all devices that have incidents related to the technical support case.
-

To collect additional information about a technical support case by executing Junos OS commands:

1. From the Service Now Navigation tree, select **Service Central > View Tech Support Cases**.

The View Tech Support Cases page appears.

2. Select the case for which you want to collect additional information.
3. Select **Collect Additional Information > Create** from the Actions list or the right-click menu.

The Collect Additional Information page appears as shown in [Figure 22 on page 87](#).

Figure 22: Collect Additional Information Page

Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: Multiple commands should be entered as , or ; or new line character.

☒ **Schedule at a later time**

Start: 05/21/17 6:25 PM IST

☒ **Repeat**

Interval: Weekly Every 1 Weeks

☒ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

Ends on: ☒ Never
☐ 05/21/17 6:25 PM IST

Submit **Cancel**

- In the CLI Commands text box, enter the commands that you want to execute to collect additional information.



NOTE: Service Now does not validate the commands that you enter to collect additional information. To add multiple commands, use comma (,) or semi-colon (;) or the new line character (press Enter on keyboard) consistently as the delimiter.

- (Optional) Select the **Schedule at a later time** check box and select the date and time the commands should be executed.



NOTE: Service Now executes the commands are executed immediately after you click Submit if you do not schedule a date and time for the commands to be executed.

- (Optional) Select the **Repeat** check box and select the time interval and the frequency of executing the commands.

The intervals can be in minutes, hours, daily, weekly, monthly, or yearly to collect additional information. By default, an interval of once a week is selected.

7. (Optional) To define an end time for collecting information for the incident, do one of the following:

- Click **Never** to continue collecting information by executing the commands at the defined interval till the incident is closed. This option is selected by default.
- Select the date and time when the commands should stop executing.

8. Click **Submit** to save the configuration or **Cancel** to cancel the configuration.

Service Now executes the job to collect additional information immediately if the job is not scheduled for a later time.

See [“Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case” on page 84](#) to check whether the job to collect additional information is successful or not.

Related Documentation

- [Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case on page 84](#)
- [Configuring Junos OS Commands to Collect Additional Information About an Incident on page 75](#)
- [Modifying the Configuration for Collecting Additional Information for a Technical Support Case on page 88](#)
- [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 90](#)
- [Downloading the Additional Information Collected for a Technical Support Case on page 91](#)
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)

Modifying the Configuration for Collecting Additional Information for a Technical Support Case

If the job to collect additional information is not already executed, you can modify the following attributes in a configuration for collecting additional information for a technical support case:

- Junos OS commands configured for execution to collect additional information
- Date and time the commands should be executed
- Interval for executing the commands if the commands are configured to be executed repeatedly

To modify the configuration for collecting additional information for a technical support case:

1. From the Service Now Navigation tree, select **Service Central > View Tech Support Case**.

The View Tech Support Cases page appears.

2. Select the case for which you want to modify configured commands.
3. Select **Collect Additional Information > Modify** from the Actions list or the right-click menu.

The Modify Collect Additional Information page appears as shown in [Figure 23 on page 89](#).



NOTE: The Modify option is disabled if the job to collect additional information is in progress or complete.

Figure 23: Modify Collect Additional Information Page

Modify Collect Additional Information

Note:-
 1) Service Now will not validate the commands entered by the user.
 2) Multiple commands should be separated using one type of delimiter. Please use either , or ; or new line character as a delimiter.

CLI Commands: show version

☒ **Schedule at a later time**

Start: 05/21/17 6:28 PM IST

☒ **Repeat**

Interval: Minutes Every 2 Minutes

Ends on: ☒ Never ☐ 05/21/17 6:28 PM IST

Submit **Cancel**

4. (Optional) Modify the commands in the **CLI Commands** text box.

5. (Optional) Modify the schedule for executing the commands under the **Schedule at a later time** section.
6. (Optional) Modify the interval at which the commands should be executed under the **Repeat** section.
7. Click **Submit**.

Service Now reschedules the job to collect additional information and displays the job ID.
8. (Optional) Click the job ID to view the job details.

The Job Details page displays the progress of the job.

Related Documentation

- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 85](#)
- [Modifying the Settings for Collecting Additional Information for an Incident on page 79](#)
- [Deleting the Configuration for Collecting Additional Information for a Technical Support Case on page 90](#)
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)

Deleting the Configuration for Collecting Additional Information for a Technical Support Case

You can delete a non-recurring configuration for collecting additional information that is scheduled to be executed later by deleting the job from the Jobs workspace of the Service Now navigation tree.

A recurring configuration can be deleted by modifying the configuration. When you modify a recurring configuration, the old configuration is deleted and a new configuration is created with the modifications. You can modify a recurring configuration even if it is already executed one or more number of times. You can delete the recurring configuration from the Jobs workspace.

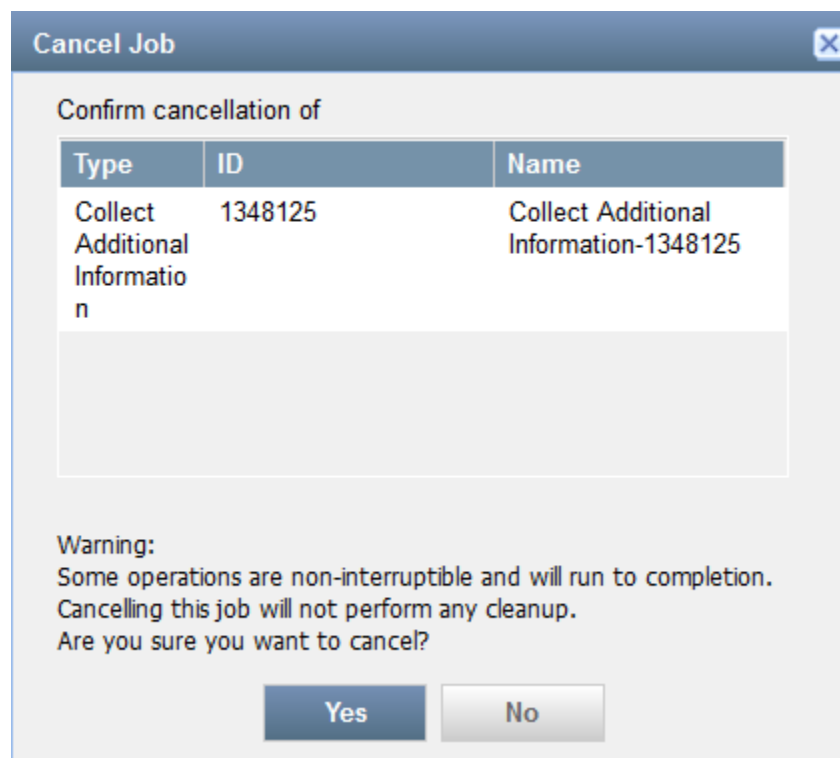
To delete a configuration for collecting additional information from the Jobs workspace:

1. On the Service Now navigation tree, click **Jobs > Job Management**.

The Job Management page appears.
2. Select the Collect Additional Information job to be deleted and click **Cancel Job** from the Actions list or the right-click menu.

A confirmation message appears as shown in [Figure 24 on page 91](#).

Figure 24: Cancel Job Dialog Box



3. Click **Yes**.

Service Now cancels the job and changes the **State** of the job to **Cancelled** from **Scheduled**.

Related Documentation

- [Deleting the Settings for Collecting Additional Information for an Incident on page 81](#)
- [Viewing Junos OS Commands Configured for Collecting Additional Information for a Technical Support Case on page 84](#)
- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 85](#)
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)

Downloading the Additional Information Collected for a Technical Support Case

You can download the additional information collected for a technical support case from the Collect Additional Information Attachment Details tab of the Tech Support Case Summary page. The Collect Additional Information Attachment Details tab of the Tech Support Case Summary tab provides the following information and the **Download all additional information attachments** link to download the attachments:

- Name of the file containing the additional information
- Size of the file (in bytes)
- User who configured the commands to be executed for collecting additional information
- Status of reading the additional information collected on a device
- Status of uploading the additional information to JSS or Service Now partner
- Remarks, if any, for the additional information collected

To download the additional information collected for a technical support case:

1. On the Service Now navigation tree, select **Service Central > View Tech Support Case**.
The View Tech Support Cases page appears.
2. Double-click the case for which you want to download additional information collected.
The Tech Support Case Summary page appears.
3. Click the **Collect Additional Information Attachment Details** tab and then click the **Download all additional command attachments** link.
Service Now generates a compressed file, in ***.zip** format, that contains outputs of the additional commands.
4. Download the attachment and save it on your local system.

**Related
Documentation**

- [Configuring Junos OS Commands to Collect Additional Information for a Technical Support Case on page 85](#)
- [Downloading the Additional Information Collected About an Incident on page 82](#)
- [Collecting Additional Information for Service Now Incidents and Cases Overview on page 74](#)

CHAPTER 6

Managing Messages

- [Service Now Messages Overview on page 93](#)
- [Assigning Ownership to Messages on page 94](#)
- [Flagging a Message to Users on page 95](#)
- [Scanning a Message for Impact on page 95](#)
- [Assigning a Message to an End Customer on page 96](#)
- [Deleting a Message on page 98](#)

Service Now Messages Overview

Service Now polls Juniper Support Systems (JSS) regularly for information messages such as notifications for JSS downtime and availability of new Service Now, Service Insight, or AI-Scripts releases for download. These information messages are displayed on the Service Now Messages page (**Service Central > Information > Messages**). Service Now allows you to assign the information message to a user for ownership and flag it to one or more users. This ensures that users are kept informed of changes made to information messages.

Associated Actions

You can perform the following actions related to messages:

- View list of information messages received from JSS
- Assign an owner to an information message; see [“Assigning Ownership to Messages” on page 94](#) for details.
- Assign messages to connected members.
- Flag an information message to users; see [“Flagging a Message to Users” on page 95](#) for details.
- Delete information messages; see [“Deleting a Message” on page 98](#) for details.
- Scan for devices impacted by the message; see [“Scanning a Message for Impact” on page 95](#) for details.

Related Documentation

- [Service Now Device Snapshots Overview on page 99](#)

- [Service Now Organizations Overview](#)

Assigning Ownership to Messages

Junos Space Service Now provides the Assign Ownership option on the Actions list to assign a user to take up ownership of the 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 95](#)
- [Scanning a Message for Impact on page 95](#)
- [Deleting a Message on page 98](#)
- [Assigning a Message to an End Customer on page 96](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Service Now Messages Overview on page 93](#)
- [Service Now Device Snapshots Overview on page 99](#)

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 Junos Space 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**.

Service Now notifies the specified users about the selected information message.

Related Documentation

- [Service Now Device Snapshots Overview on page 99](#)
- [Assigning Ownership to Messages on page 94](#)
- [Scanning a Message for Impact on page 95](#)
- [Deleting a Message on page 98](#)
- [Assigning a Message to an End Customer on page 96](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Service Now Messages Overview on page 93](#)

Scanning a Message for Impact

You can use Junos Space 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**

- [Service Now Device Snapshots Overview on page 99](#)
- [Assigning Ownership to Messages on page 94](#)
- [Flagging a Message to Users on page 95](#)
- [Deleting a Message on page 98](#)
- [Assigning a Message to an End Customer on page 96](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Service Now Messages Overview on page 93](#)

Assigning a Message to an End Customer

Junos Space Service Now polls Juniper Support Systems (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 Direct, 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:

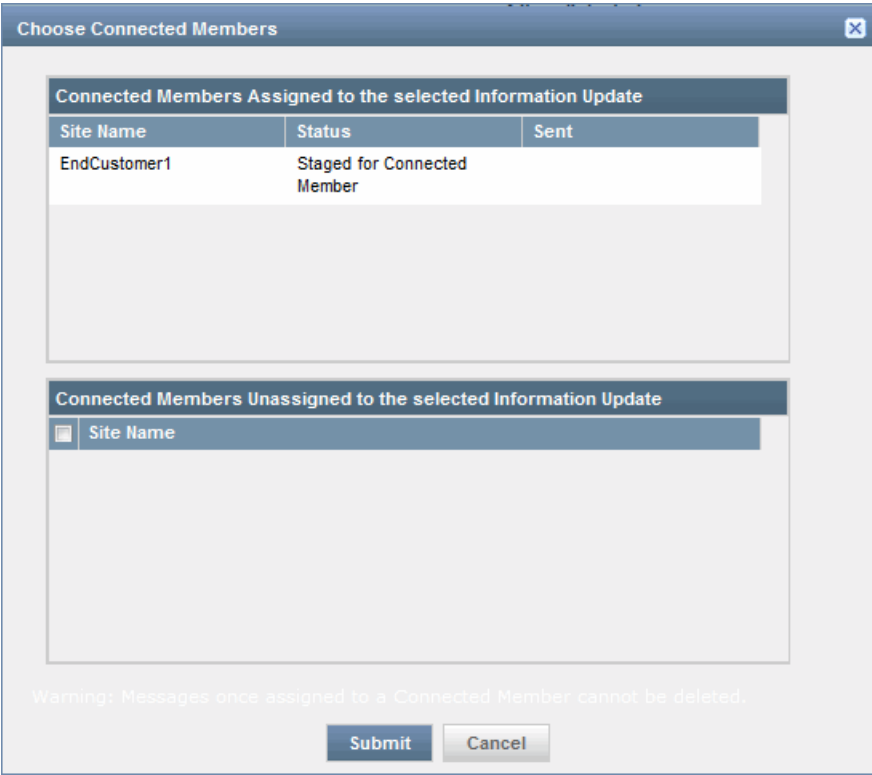
1. From the Service Now navigation tree, select **Service Central > Information > Messages**.

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 25 on page 97](#), 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 25: 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 label "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](#)
- [Service Now Device Snapshots Overview on page 99](#)
- [Assigning Ownership to Messages on page 94](#)
- [Flagging a Message to Users on page 95](#)
- [Scanning a Message for Impact on page 95](#)
- [Deleting a Message on page 98](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Service Now Messages Overview on page 93](#)

Deleting a Message

Junos Space Service Now provides the Delete option on the Actions list to delete information messages from the Service Now database.

To delete an information message:

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

The Messages page appears.

2. Select one or more 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.

Service Now deletes the selected information messages from the Service Now database and removes them from the Messages page.

Related Documentation

- [Service Now Device Snapshots Overview on page 99](#)
- [Assigning Ownership to Messages on page 94](#)
- [Flagging a Message to Users on page 95](#)
- [Scanning a Message for Impact on page 95](#)
- [Assigning a Message to an End Customer on page 96](#)
- [Viewing Messages Assigned to an End Customer](#)
- [Service Now Messages Overview on page 93](#)

CHAPTER 7

Managing Device Snapshots or iJMBs

- [Service Now Device Snapshots Overview on page 99](#)
- [Viewing Details of a Device Snapshot on page 100](#)
- [Exporting Device Snapshots to HTML on page 102](#)
- [Deleting Device Snapshots on page 103](#)

Service Now Device Snapshots Overview

Junos Space Service Now periodically collects device snapshots [also known as informational Juniper Message Bundles (iJMBs)] that contain configuration and trend information of devices. Service Now displays the iJMBs on the Device Snapshot page (**Service Central > Information > Device Snapshots**). By default, Service Now sends the iJMBs to Juniper Support Systems (JSS) or Service Now Partner for processing. 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 if the device is susceptible to known issues.

If AI-Scripts is installed on a device, device snapshots are generated once every 7 days. Service Now collects the device snapshot and shares it with JSS or Service Now partner for analysis. Before sharing the device snapshots, Service Now filters the configuration information in the device snapshot based on the **JMB Filter Level** set for the organization to which the devices belongs. For information about JMB filter levels, see *Adding an Organization to Service Now*

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.

When Service Now detects that a device has not generated iJMB for more than seven days, it generates on-demand device snapshots by using the **directive.rc** file and shares it with JSS or Service Now partner. Service Now also detects devices that have stopped

sending device snapshots for more than two weeks and displays them graphically on the Administration page. To view details of such devices, you can click the Devices Not Sending Snapshots bar of the Devices Not Sending Device Snapshots graph. Service Now opens the Service Now Devices page where you can view their details and export the device details to an Excel file.

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; SNMP traps are not sent.

Associated Actions

You can perform the following actions related to device snapshots:

- Export device snapshots in HTML format; see [“Exporting Device Snapshots to HTML” on page 102](#) for details.
- Delete device snapshots; see [“Deleting Device Snapshots” on page 103](#) for details.
- View device snapshots; see [“Viewing Details of a Device Snapshot” on page 100](#) for details.

Related Documentation

- [Service Now Messages Overview on page 93](#)
- [Monitoring Device Snapshots](#)
- [Adding an Organization to Service Now](#)
- [AI-Scripts Overview](#)

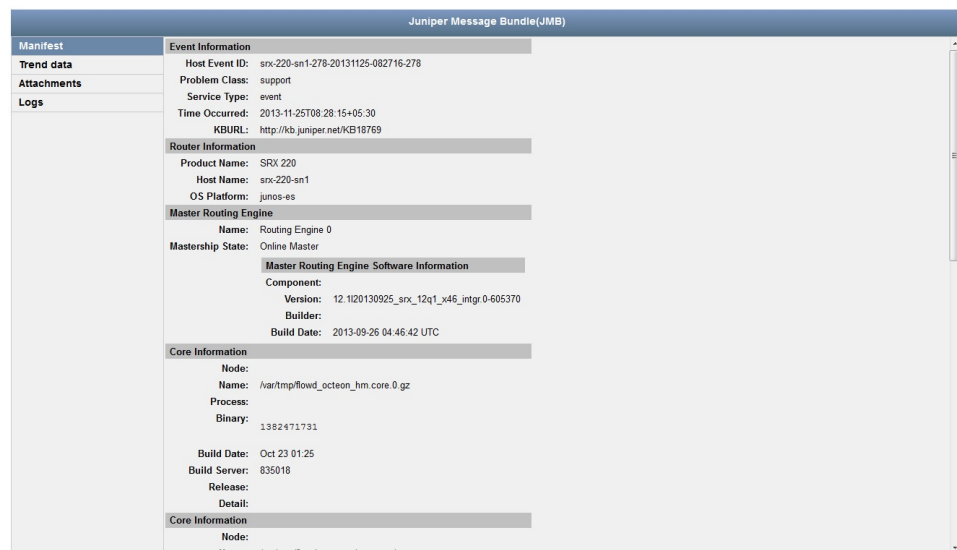
Viewing Details of a Device Snapshot

When Junos Space 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 26 on page 101](#). You can click the links in the Attachments and Logs sections to view or download attachments and system log files.

Figure 26: Juniper Message Bundle

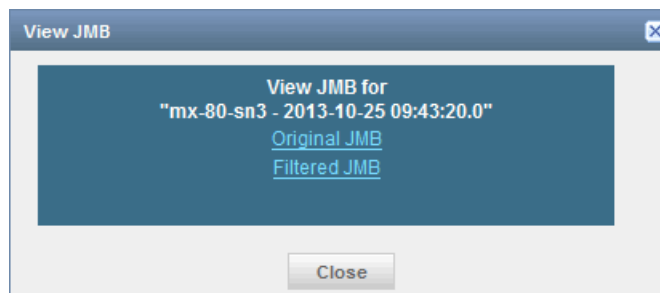


To view details of a JMB:

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 list, 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 27 on page 101](#). The information in the filtered JMB is displayed based on the JMB filter level set for the organization associated with the device for which the JMB is generated.

Figure 27: 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 defined by the JMB filter level set for the organization associated with the device for which the JMB is generated.

- Related Documentation**
- [Service Now Device Snapshots Overview on page 99](#)
 - [Exporting Device Snapshots to HTML on page 102](#)
 - [Deleting Device Snapshots on page 103](#)
 - [Service Now Messages Overview on page 93](#)

Exporting Device Snapshots to HTML

Junos Space Service Now provides the Export iJMB to HTML option in the Actions list of the Device Snapshots page to export device snapshots collected by Service Now in HTML format. Service Now exports iJMBs as a zipped folder. The view of the exported JMB file is the same as that of the Juniper Message Bundle (JMB) page in Service Now.

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 device snapshot that you want to export, and select **Export iJMB 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**
- [Service Now Device Snapshots Overview on page 99](#)
 - [Deleting Device Snapshots on page 103](#)
 - [Viewing Details of a Device Snapshot on page 100](#)
 - [Service Now Messages Overview on page 93](#)

Deleting Device Snapshots

Junos Space 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 configurable on the Device Snapshot Purge Time (in days) parameter on the Global Settings page. For information about configuring a purge time for device snapshots, see *Configuring Global Settings*.

Service Now provides the Delete option on the Actions list on the Device Snapshots page to delete device snapshots 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 device snapshot 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.

Service Now deletes the device snapshot from the Service Now database and removes them from the Device Snapshots page.

Related Documentation

- [Service Now Device Snapshots Overview on page 99](#)
- [Exporting Device Snapshots to HTML on page 102](#)
- [Viewing Details of a Device Snapshot on page 100](#)
- [Service Now Messages Overview on page 93](#)
- [Junos Space Service Now Global Settings Overview](#)

CHAPTER 8

Managing BIOS Validations

- [Service Now BIOS Validation Overview on page 105](#)
- [Viewing BIOS Validations on page 107](#)
- [Exporting BIOS Validation Results on page 109](#)
- [Deleting BIOS Validation Incidents on page 110](#)

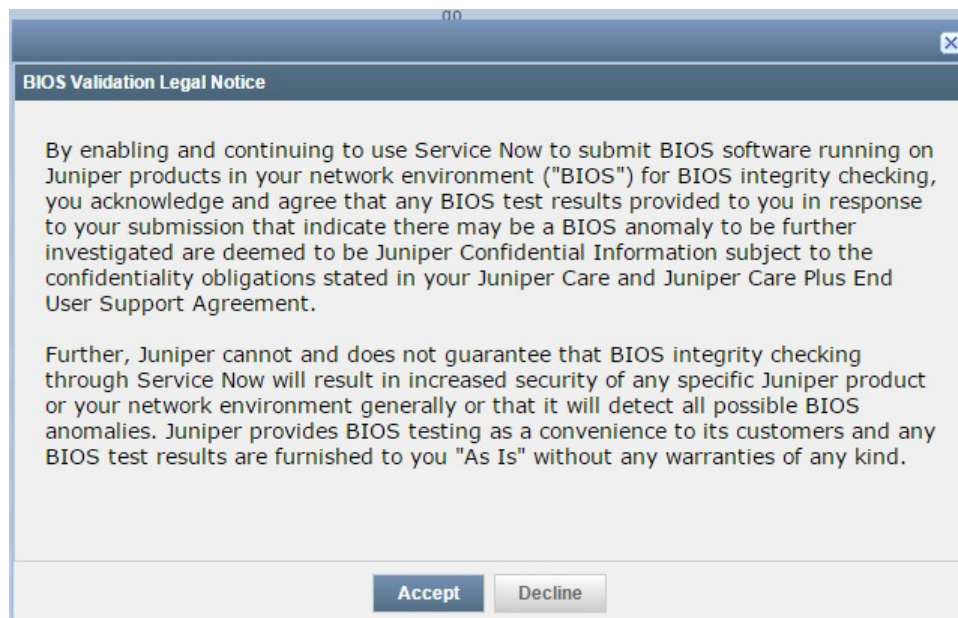
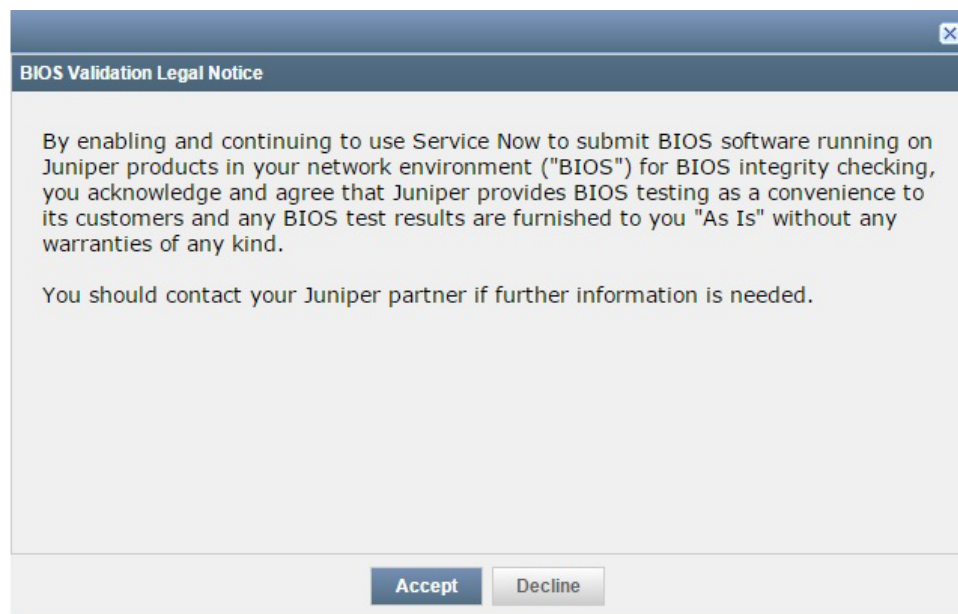
Service Now BIOS Validation Overview

Junos Space Service Now provides the BIOS validation option to 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, Service Now creates BIOS validation incidents (**Service Central > Device Analysis > BIOS Validations**) and submits the BIOS data to Juniper Support Systems (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 28 on page 106](#) and [Figure 29 on page 106](#) show the legal notice displayed on Service Now operating in Partner Proxy and End Customer modes respectively.

Figure 28: BIOS Validation Legal Notice on Service Now Partner*Figure 29: BIOS Validation Legal Notice on Service Now End Customer*

Associated Actions

You can perform the following actions related to BIOS validation:

- View BIOS validation incidents; see [“Viewing BIOS Validations”](#) on page 107 for details.
- Export BIOS validation incidents; see [“Exporting BIOS Validation Results”](#) on page 109 for details.

- Delete BIOS validation incidents; see [“Deleting BIOS Validation Incidents” on page 110](#) for details.

**Related
Documentation**

- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device](#)
- [Service Now Product Health Data Collection Overview on page 113](#)

Viewing BIOS Validations

On its dashboard, the Device Analysis task displays the status and results of the BIOS validations for all managed devices. Junos Space 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 9 on page 107](#) lists the information displayed by the BIOS validations report.

Table 9: 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.

Table 9: BIOS Validations Field Descriptions (continued)

Field Name	Description
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	
Attachment	<p>Name of the attachment file</p> <p>You cannot view the contents of the attachment file.</p>
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	<p>The system log file collected as part of BIOS validation</p> <p>You cannot view the contents of the system log files.</p>
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 Incidents” on page 110](#)

- Export information about BIOS validation results to Excel, see [“Exporting BIOS Validation Results” on page 109](#)

**Related
Documentation**

- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device](#)
- [Service Now Product Health Data Collection Overview on page 113](#)

Exporting BIOS Validation Results

You can export the details of BIOS validation incidents of managed devices to an Excel file for reference. [Table 10 on page 109](#) lists the BIOS validation information exported to an Excel file.

Table 10: 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
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 Systems (JSS) or Service Now partner for validation. • Submitted—Service Now has submitted the BIOS data for validation. • Submission Failed—Service Now is unable to submit the BIOS data. for validation • Validation Success—Validation of BIOS data 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 or Service Now
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 details:

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 list, 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**

- [Service Now BIOS Validation Overview on page 105](#)
- [Configuring BIOS Validation for Verifying BIOS Integrity of a Device](#)
- [Viewing BIOS Validations on page 107](#)
- [Deleting BIOS Validation Incidents on page 110](#)

Deleting BIOS Validation Incidents

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 incident if the status of BIOS validation 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 incidents to be deleted.

3. From the Actions list, 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 incident or **Cancel** to cancel the deletion.

If you click Delete, Service Now deletes the BIOS validation incidents and removes them from the BIOS Validations page.

**Related
Documentation**

- [Service Now BIOS Validation Overview on page 105](#)
- [Viewing BIOS Validations on page 107](#)
- *Configuring BIOS Validation for Verifying BIOS Integrity of a Device*
- [Exporting BIOS Validation Results on page 109](#)

CHAPTER 9

Analyzing Physical Health Data

- [Service Now Product Health Data Collection Overview on page 113](#)
- [Exporting Product Health Data Information to an Excel File on page 115](#)
- [Viewing Product Health Data Files Collected from a Device on page 120](#)
- [Deleting Product Health Data Files Collected from a Device on page 124](#)

Service Now Product Health Data Collection Overview

Starting from Service Now Release 15.1R1, Service Now collects product health data (PHD) from managed devices to assess the health of the devices.



NOTE:

- PHDC is not supported on Service Now operating in End Customer mode.
Starting in Service Now Release 16.1R1, a Service Now partner can collect PHD on end-customer devices.
- 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 is composed of 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 120](#).

[Figure 30 on page 114](#) shows the Product Health Data Devices page that lists the devices from which Service Now collects PHD. You can view the status of PHD collected on a

device on this page. Service Now lists a device on this page when at least one PHD file is collected from it.

Figure 30: Product Health Data Devices Page

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

Table 11 on page 114 describes the fields on the Product Health Data Devices page.

Table 11: 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	Link to view the PHD files collected from the device For information about viewing the PHD files, see “Viewing Product Health Data Files Collected from a Device” on page 120.

Service Now submits the PHD collected to Juniper Support Systems (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 115](#).

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16.1R1, a Service Now partner can collect PHD on end-customer devices
15.1R1	Starting from Service Now Release 15.1R1, Service Now collects product health data (PHD) from managed devices to assess the health of the devices

Related Documentation

- *Product Health Data Collection Configuration Overview*
- [Service Now BIOS Validation Overview on page 105](#)

Exporting Product Health Data Information to an Excel File

Junos Space Service Now provides the Export and Export All options in the Actions list of the Product Health Data Devices page 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 31 on page 115](#) shows a sample of the information about devices exported to Excel.

Figure 31: PHDC Information of Devices Exported to Excel

	A	B	C	D	E	F	G	H
1	Device	Serial Number	PHD Group Name	Start Date	Status	Total Files Received	Last Uploaded	Status Message
2	mx-80-an2	D4358	Test-group	2015-07-16 01:32:51.36	Running	28		
3	mx-480-an1	JN11AFF42AFB	Test-group	2015-07-16 01:32:51.36	Running	28		
4								
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 was created.

Figure 32 on page 116 shows a sample of the information about PHD files exported to Excel.

Figure 32: 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 10:18:08.19	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 116](#)
- [Exporting Data about PHD Files Collected from a Device on page 118](#)

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, Service Now exports information about all the managed devices in Service Now from which PHD is collected; whereas, when you export information about devices from the Product Health Data Collection task in the Administration workspace Service Now exports, information about devices in the selected PHDC configuration.

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 33 on page 117](#). The View all Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 33: View all Devices of this PHDC

Device	Serial Number	Product	Start Date	Status	Total Files Available
sn-220-sn1	AQ5210AA0078	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

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

Service Now displays the Export All Product Health Data Devices dialog box. 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**.

Service Now displays the Export Selected Product Health Data Devices dialog box. 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 34 on page 119](#).

Figure 34: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_162001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_2015_0416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sn1_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 35 on page 119](#). The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 35: View All Devices of this PHDC Page

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

- 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**.

Service Now displays the Export All Product Health Data Information dialog box. 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**.

Service Now displays the Export Selected Product Health Data Information dialog box. 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

- [Service Now Product Health Data Collection Overview on page 113](#)
- [Viewing Product Health Data Files Collected from a Device on page 120](#)
- *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. Service Now uploads these files to Juniper Support Systems (JSS) for assessment. You can view the list of PHD files collected for a device on the View all Product Health Data Files page as shown in [Figure 36 on page 121](#). You can also download, export, and delete the PHD files by using this page.

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

Figure 36: View All Product Health Data Files Page

File Name	PHDC Name	Received	File Size (Bytes)	Read Status	Upload Status
ex-4200-sn1_phdc_jmb_ais_health_20150416_182001.bt	EX Group	Aug 7, 2015 4:12:19 PM IST	21460	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_20150416_172000.bt	EX Group	Aug 7, 2015 3:12:16 PM IST	21459	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_20150416_162002.bt	EX Group	Aug 7, 2015 2:12:19 PM IST	21325	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_20150416_152001.bt	EX Group	Aug 7, 2015 1:12:20 PM IST	21188	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_20150416_142001.bt	EX Group	Aug 7, 2015 12:12:20 PM IST	21324	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_20150416_132000.bt	EX Group	Aug 7, 2015 11:12:19 AM IST	44968	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_20150416_122000.bt	EX Group	Aug 7, 2015 10:12:18 AM IST	21188	Success	Uploaded
ex-4200-sn1_phdc_jmb_ais_health_20150416_112000.bt	EX Group	Aug 7, 2015 9:12:19 AM IST	21459	Success	Uploaded

Table 12: 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: <i>hostname-sys_phdc_jmb_ais_health_yyyymmdd_hhmmss</i>, where</p> <ul style="list-style-type: none"> <i>hostname</i> is the hostname of the device from which PHD is collected. <i>yyymmdd</i> is the date when PHD was collected. <i>hhmmss</i> 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 it is collected 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.

Table 12: Fields on the View All Product Health Data Files Page (continued)

Field Name	Description
Upload Status	Status of uploading PHD files to JSS: <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 37 on page 123](#).

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

Figure 37: View All Devices of this PHDC Page

Device	Serial Number	Product	Start Date	Status	Total Files Available
snv-220-sn1	AG5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0
snv-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 a 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

- [Service Now Product Health Data Collection Overview on page 113](#)
- [Product Health Data Collection Configuration Overview](#)
- [Exporting Product Health Data Information to an Excel File on page 115](#)
- [Deleting Product Health Data Files Collected from a Device on page 124](#)
- [Deleting a Product Health Data Collection Configuration from Service Now](#)

Deleting Product Health Data Files Collected from a Device

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

Service Now provides the Delete option to delete the PHD files if you choose to do so. 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 38 on page 125](#).

Figure 38: View All Product Health Data Files Page

Applications > Service Central > Device Analysis > Product Health Data Devices > View all Product Health Data Files						
Back						
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 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 39 on page 125](#).

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

Figure 39: View All Devices of this PHDC Page

Applications > Administration > Product Health Data Collection > View all Devices of this PHDC						
Back						
Device	Serial Number	Product	Start Date	Status	Total Files Available	
srn-220-sr1	AQ5210AA0078	SRX220H	Aug 27, 2015 10:16:00 AM IST	Running	0	
srn-650-sr2	AJ4410AA0037	SRX650	Aug 27, 2015 10:16:00 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, Service Now displays a message indicating that the files are deleted.

**Related
Documentation**

- [Service Now Product Health Data Collection Overview on page 113](#)
- [Product Health Data Collection Configuration Overview](#)
- [Viewing Product Health Data Files Collected from a Device on page 120](#)
- [Exporting Product Health Data Information to an Excel File on page 115](#)

CHAPTER 10

Managing JMB with Errors

- [JMBs with Errors on page 127](#)

JMBs with Errors

Junos Space 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 erroneous JMBs 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 127](#)
- [Deleting JMBs with Errors on page 128](#)

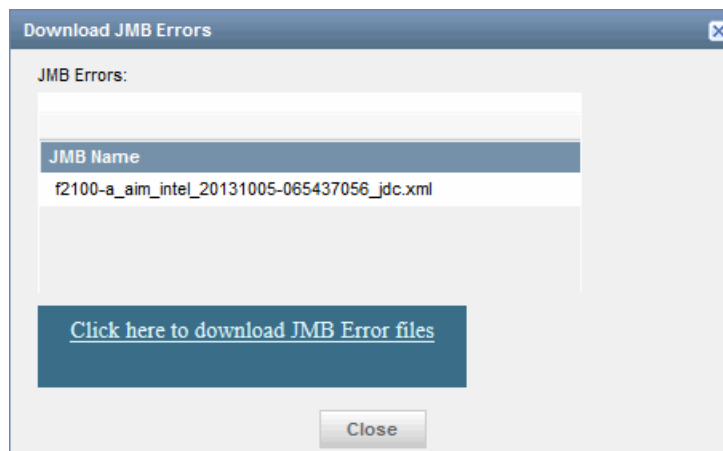
Downloading JMBs with Errors

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

To download erroneous JMBs:

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 (upto five JMBs) that you want to download.
3. From the Actions list, 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 40 on page 128](#).

Figure 40: 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.

See Also

Deleting JMBs with Errors

You can delete multiple erroneous JMBs 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 list, select **Delete**. Alternatively, right-click and select **Delete**.

Service Now displays the Delete Error JMB dialog box and 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](#)
- [Service Now Messages Overview on page 93](#)

CHAPTER 11

Viewing and Managing Suppressed Events

- [Service Now Suppressed Events Overview](#) on page 131
- [Viewing Details of JMBs for Suppressed Events](#) on page 132
- [Creating Incidents for Suppressed Juniper Message Bundles](#) on page 132
- [Deleting JMBs for Suppressed Events](#) on page 134

Service Now Suppressed Events Overview

Suppressed Events are events for which Junos Space Service Now does not create incidents as the JMBs for the events are filtered by incident filters. Starting in Junos Space Service Now Release 17.1R1, you can view events that were suppressed on the Suppressed Events page (**Service Central > Suppressed Events**) and, if required, create incidents for the suppressed events.

[Figure 41 on page 131](#) shows the Suppressed Events page .

Figure 41: Suppressed Events Page

Organization	Device Group	Received Time	Device	Event Name	JMB Name	Problem Identifier
Prod_Org	Default for TestORG	May 17, 2017 6:58:46 PM IST	sn-space-ex4550-sys	CHASSISD_CFEED_POWER_FAIL_URE	sn-space-ex4550-sys_20170516_142502_411_jmb	sn-space-ex4550-sys-411-20170516-142311-4_ala_prob.xml

Associated Actions

You can perform the following actions related to suppressed events:

- Delete JMBs for suppressed events; see [“Deleting JMBs for Suppressed Events”](#) on [page 134](#) for details.
- View JMBs for suppressed events; see [“Viewing Details of JMBs for Suppressed Events”](#) on [page 132](#) for details.
- Create incident for the suppressed events; see [“Creating Incidents for Suppressed Juniper Message Bundles”](#) on [page 132](#) for details.

Related Documentation

- [Service Now Incident Filters Overview](#)
- [Service Now Auto Submit Filters Overview](#)

Viewing Details of JMBs for Suppressed Events

You can view the details of the JMBs that were filtered by incident filters defined to not create incidents on the Suppressed Events page. The Suppressed Events page displays the following information about a JMB:

- Organization—The organization with which the JMB is associated
- Device Group—The device group with which the device from which the JMB was generated is associated
- Received Time—The date and time the JMB was received by Service Now
- Device—The device from which the JMB was generated
- Event Name—The event that triggered the generation of JMB
- JMB Name—The name of the JMB
- Problem Identifier—The ID of the event that occurred on the device
- Filter—The filter used to suppress incident creation for the JMB
- Product—The Juniper Networks product on which the JMB was created
- Priority—Priority of the event

To view details of JMBs for suppressed events:

1. In the Service Now navigation tree, click **Service Central > Suppressed Events**.

The Suppressed Events page appears.

2. Select a JMB for viewing details.

The JMB details page appears. For information about details about JMB, see *Contents of a JMB*.

Related Documentation

- [Service Now Suppressed Events Overview on page 131](#)
- [Creating Incidents for Suppressed Juniper Message Bundles on page 132](#)
- [Deleting JMBs for Suppressed Events on page 134](#)

Creating Incidents for Suppressed Juniper Message Bundles

You can create incidents for JMBs suppressed by incident filters. This option is helpful when you have exceptions to incident filters that are defined to not create incidents.

To create incidents for suppressed JMBs:

1. In the Service Now navigation tree, click **Service Central > Suppressed Events**.

The Suppressed Events page appears.

2. Select one or more JMBs for which you want to create incidents and select **Create Incident** from the Actions list or the right-click menu.

The Create Incident Suppressed JMBs dialog box appears as shown in [Figure 42 on page 133](#).

Figure 42: Create Incident for Suppressed JMBs Dialog Box



3. Click **Create**.

The Create Incident for Suppressed JMBs dialog box appears.

4. Click **Create**.

Service Now creates a new incident and lists it on the Incidents page. The JMB is removed from the Suppressed Events page.

Related Documentation

- [Service Now Suppressed Events Overview on page 131](#)
- [Viewing Details of JMBs for Suppressed Events on page 132](#)
- [Deleting JMBs for Suppressed Events on page 134](#)

Deleting JMBs for Suppressed Events

Junos Space Service Now provides the Delete option in the Actions list of the Suppressed Event page to delete JMBs for which incidents are not created.

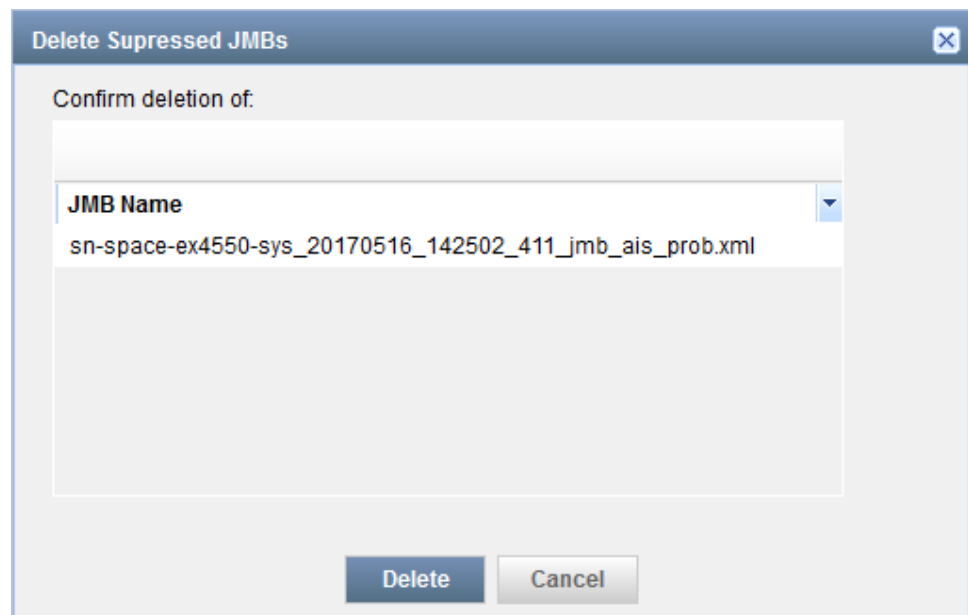
1. In the Service Now navigation tree, click **Service Central > Suppressed Events**.

The Suppressed Events page appears.

2. Select one or more JMBs that you want to delete and select **Delete** from the Actions list or the right-click menu.

The Delete Suppressed Events dialog box appears as shown in [Figure 43 on page 134](#).

Figure 43: Delete Suppressed Events Dialog Box



3. Click **Delete**.

The selected JMBs are deleted and are not listed on the Suppressed Events page.

Related Documentation

- [Viewing Details of JMBs for Suppressed Events on page 132](#)
- [Service Now Suppressed Events Overview on page 131](#)
- [Creating Incidents for Suppressed Juniper Message Bundles on page 132](#)

CHAPTER 12

Managing Notifications

- [Service Now Notification Policies Overview on page 135](#)
- [Creating and Editing a Notification Policy on page 137](#)
- [Enabling or Disabling a Notification Policy on page 146](#)
- [Deleting a Notification Policy on page 146](#)

Service Now Notification Policies Overview

Junos Space 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, such as new incident created, a case created for the incident, or a device snapshot received, for which you want Service Now to send a notification.

You can view notification policies configured in Service Now on the Notifications page (**Service Central > Notifications**).

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

- **Trigger**—The event (for example, device snapshot received for a device) that causes Service Now to send notification
- **Filters**—Filters for the events that cause Service Now to send a notification
- **Actions**—List of user e-mail IDs and SNMP trap destinations to which the notifications must be sent when the event occurs..

[Table 13 on page 135](#) lists the triggers and filters that can be configured on Service Now.

Table 13: 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

Table 13: Notification Triggers and Trigger Filters (continued)

Trigger	Description	Filters
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
Case ID Assigned	Trigger to send a notification when a case ID is assigned to an incident in Juniper Support Systems (JSS) or Service Now partner	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 JSS or Service Now partner 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 from a device 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

Associated Actions

You can perform the following actions related to notifications:

- Edit filters and actions configured for a trigger; see [“Creating and Editing a Notification Policy” on page 137](#) for details.
- Enable or disable a notification policy; see [“Enabling or Disabling a Notification Policy” on page 146](#) for details.
- Delete a notification policy; see [“Deleting a Notification Policy” on page 146](#) for details.

Related Documentation

- [Service Now Incidents Overview on page 37](#)
- [Service Now Technical Support Cases and End Customer Support Cases Overview on page 63](#)
- [Service Now Messages Overview on page 93](#)
- [Service Now Device Snapshots Overview on page 99](#)
- [Service Now BIOS Validation Overview on page 105](#)
- [Service Now Product Health Data Collection Overview on page 113](#)
- *Service Now E-Mail Templates Overview*

Creating and Editing a Notification Policy

Notification policies specify when you want Junos Space 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 define the trigger events, and the users and the SNMP trap destinations to which you want the notifications should be sent.

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 44 on page 138](#),

Figure 44: Create Notifications Page

2. In the **Name** text field, enter a name for the 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. From the **Trigger** list, select an event in Service Now for which you want to send notifications.

For the list of triggers, see [Table 13 on page 135](#).

4. Expand the Apply Filters section if not already expanded, and enter values for the filter parameters.

The filter parameters displayed depend on the trigger you chose in the Trigger list.

5. Under the Actions section, enter the e-mail IDs of users to whom a notification must be sent for the selected trigger.

Use the Add Email and Delete buttons to add and delete e-mail IDs.

6. Under the Send SNMP Traps to section, select the destination where SNMP traps must be sent for the selected trigger.
7. Select the **Send JMB file as attachment in mail** check box if you want the JMB to be attached to the notification e-mail.
8. Click **Add**.

Service Now creates the notification policy and lists it 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 14 on page 140](#).

Table 14: Create Notification Policy Page Field Descriptions

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

Table 14: 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 14: 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 14: 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 14: 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 14: 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 14: 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**
- [Service Now Notification Policies Overview on page 135](#)
 - [Enabling or Disabling a Notification Policy on page 146](#)
 - [Deleting a Notification Policy on page 146](#)

Enabling or Disabling a Notification Policy

Notification policies specify the events for which Junos Space 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**
- [Service Now Notification Policies Overview on page 135](#)
 - [Creating and Editing a Notification Policy on page 137](#)
 - [Deleting a Notification Policy on page 146](#)

Deleting a Notification Policy

A notification policy specifies the events for which Junos Space 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 one or more notification policies 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**.

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

**Related
Documentation**

- [Service Now Notification Policies Overview on page 135](#)
- [Creating and Editing a Notification Policy on page 137](#)
- [Enabling or Disabling a Notification Policy on page 146](#)

Trouble Ticketing

- [Setting up Java Based Web Service Client on page 149](#)
- [Accessing a Web Service on page 154](#)

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.HttpsURLConnection;
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 157](#)
- [Trouble Ticket APIs Supported by Service Now on page 158](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Accessing a Web Service on page 154](#)
- [Profiles Used by Service Now on page 158](#)
- [Error Messages Displayed by OSS/J Client on page 163](#)

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 username 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 services 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 157](#)
- [Trouble Ticket APIs Supported by Service Now on page 158](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Setting up Java Based Web Service Client on page 149](#)
- [Profiles Used by Service Now on page 158](#)
- [Error Messages Displayed by OSS/J Client on page 163](#)

CHAPTER 14

Trouble Ticket API

- [Trouble Ticket APIs Overview on page 157](#)
- [Profiles Used by Service Now on page 158](#)
- [Trouble Ticket APIs Supported by Service Now on page 158](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Error Messages Displayed by OSS/J Client on page 163](#)

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 <https://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 158](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Setting up Java Based Web Service Client on page 149](#)
- [Profiles Used by Service Now on page 158](#)
- [Accessing a Web Service on page 154](#)
- [Error Messages Displayed by OSS/J Client on page 163](#)

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 157](#)
- [Trouble Ticket APIs Supported by Service Now on page 158](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Setting up Java Based Web Service Client on page 149](#)
- [Accessing a Web Service on page 154](#)
- [Error Messages Displayed by OSS/J Client on page 163](#)

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 15: 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 by using the given key and returns only the requested attributes
<code>getTroubleTicketsByKeys</code>	Obtains multiple trouble tickets by using the given keys and returns only the requested attributes
<code>setTroubleTicketByValue</code>	Updates a single trouble ticket by 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 157](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Setting up Java Based Web Service Client on page 149](#)
- [Profiles Used by Service Now on page 158](#)
- [Accessing a Web Service on page 154](#)

- [Error Messages Displayed by OSS/J Client on page 163](#)

Trouble Ticket Attributes Supported by Service Now

The following table lists the attributes supported by Service Now.

Table 16: 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

Table 16: Supported Trouble Ticket Attributes (continued)

Trouble Ticket Attribute	Description	Access Right Provided to an External System
closeOutVerification	Indicates whether the customer has verified the resolution, denied the resolution, or taken no action.	Write access
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 157](#)
- [Trouble Ticket APIs Supported by Service Now on page 158](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Setting up Java Based Web Service Client on page 149](#)
- [Profiles Used by Service Now on page 158](#)
- [Accessing a Web Service on page 154](#)
- [Error Messages Displayed by OSS/J Client on page 163](#)

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 160. 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 160. 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 157](#)
- [Trouble Ticket APIs Supported by Service Now on page 158](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Setting up Java Based Web Service Client on page 149](#)
- [Profiles Used by Service Now on page 158](#)
- [Accessing a Web Service on page 154](#)

- [Error Messages Displayed by OSS/J Client on page 163](#)

Error Messages Displayed by OSS/J Client

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

Table 17: 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 17: 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 157](#)
- [Trouble Ticket APIs Supported by Service Now on page 158](#)
- [Trouble Ticket Attributes Supported by Service Now on page 160](#)
- [Trouble Ticket Events Supported by Service Now on page 161](#)
- [Setting up Java Based Web Service Client on page 149](#)
- [Accessing a Web Service on page 154](#)
- [Profiles Used by Service Now on page 158](#)

