



Junos[®] Space

Service Now User Guide

Release
12.1



Published: 2012-05-17

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

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

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

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

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

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

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

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

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

Junos Space Service Now User Guide
Release 12.1
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

Revision History
May 2012— Junos Space Service Now User Guide, Release 12.1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xi
	Junos Space Documentation and Release Notes	xi
	Documentation Conventions	xi
	Documentation Feedback	xii
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xiii
	Opening a Case with JTAC	xiii
Part 1	Overview	
Chapter 1	Service Now Overview	3
	Service Now Overview	3
Chapter 2	Quick Start Guide to Service Now	7
	Service Now Quick Start	7
	Downloading the Junos Space VM image	7
	Setting Up Junos Space	8
	Setting Up Service Now in Standard Mode	9
	Setting Up Service Now in partner-proxy Mode	10
Chapter 3	Upgrading Service Now	13
	Upgrading Service Now	13
Chapter 4	Service Now MIBs	17
	Service Now MIBs	17
Chapter 5	Service Now Modes	19
	Service Now Modes	19
	Overview	19
	Activating Offline, End-Customer and Partner-Proxy Modes	21
Chapter 6	Service Now Dashboard and Workspaces Overview	23
	Service Now Dashboard Overview	23
	Service Now Workspaces	23
	Dashboard Gadgets	24
	Platforms with Most Incidents	25
	Devices with the Most Incidents	25
	Service Now Notices (Upgrade and Contract Notice)	25
Chapter 7	Service Now Icons	27
	Service Now Icons	27
Chapter 8	User Roles	31
	Service Now User Roles	31

Part 2	Using the Service Now Getting Started Assistant	
Chapter 9	Service Now Getting Started Assistant Usage Overview	37
	Service Now Getting Started Assistant Usage Overview	37
Part 3	Administration	
	Administration Overview	39
Chapter 10	Organizations	41
	Organizations Overview	41
	Adding an Organization	43
	Adding a Connected Member	46
	Modifying Organization Parameters	47
	Deleting an Organization	48
	Test the Connection to JSS	48
	Viewing Messages Assigned to a Connected Member	49
	Running an Organization in Test Mode	50
Chapter 11	Device Groups	51
	Device Groups Overview	51
	Creating a Device Group	51
	Modifying Device Groups	52
	Deleting Device Groups	53
Chapter 12	Service Now Devices	55
	Service Now Devices Overview	55
	Adding Devices from the Platform	58
	Installing an Event Profile on Devices Using Service Now	59
	Manually Installing AI-Scripts on Devices	62
	Uninstalling Event Profiles from Devices	63
	Exporting Device Data in CSV and Excel Format	63
	Exporting Inventory Information in CSV Format	64
	Viewing Exposure	64
	Generating On-Demand Incidents	65
	Deleting a Device	67
	Associating Devices with a Device Group	68
	Adding Devices to Auto Submit Policies	69
Chapter 13	Event Profiles and AI-Scripts	71
	Event Profiles Overview	71
	Adding an Event Profile	73
	Cloning an Event Profile	78
	Deleting Event Profiles	79
	Viewing an Event Profile	80
	Pushing an Event Profile to Devices	80
	Displaying Devices Associated with an Event Profile	83
	Setting an Event Profile as Default	83
	Exporting Events Data in Excel Format	84

	AI-Scripts Overview	85
	What AI-Scripts Do	85
	Events Detected by AI-Scripts	86
	JMB Contents	87
	Adding a Script Bundle to Service Now	87
	Setting a Script Bundle as Default	88
	Deleting a Script Bundle from Service Now	88
Chapter 14	Global Settings	91
	Configuring Global Settings	91
	Adding an SNMP Server	94
	Editing and Deleting an SNMP Server	96
	Configuring Proxy Server Settings	96
Chapter 15	Auto Submit Policy	99
	Auto Submit Policy Overview	99
	Creating an Auto Submit Policy	100
	Modifying an Auto Submit Policy	103
	Deleting Auto Submit Policies	104
	Exporting Incidents Report	104
	Changing the Status of Auto Submit Policies	105
Part 4	Service Central	
	Service Central Overview	107
Chapter 16	Incidents	109
	Incidents Overview	109
	Assigning an Incident Owner	111
	Flagging an Incident to a User	112
	Checking Incident Status Updates	113
	Exporting Incident Data	114
	Deleting an Incident	115
	Submitting an Incident to Juniper Support Systems	115
	Viewing Incident Details	117
	Viewing Knowledge Base Articles Associated with an Incident	118
	Viewing a Case in the Case Manager	118
	Updating an End-Customer Case	119
Chapter 17	Information	121
	Messages Overview	121
	Assigning Ownership	122
	Flagging a Message to Users	122
	Deleting a Message	123
	Scanning a Message for Impact	124
	Assigning a Message to a Connected Member	124
	Device Snapshots Overview	125
	Exporting Device Data into HTML	127
	Deleting Device Snapshots	127
	Viewing Device Snapshot Details	128

Chapter 18	JMB Errors	129
	JMB Errors	129
	Downloading JMB Errors	129
	Deleting JMB Errors	130
Chapter 19	Notifications	131
	Notification Policies Overview	131
	Creating and Editing a Notification Policy	132
	Enabling or Disabling a Notification Policy	137
	Deleting a Notification Policy	138
Part 5	Index	
	Index	141

List of Figures

Part 1	Overview	
Chapter 6	Service Now Dashboard and Workspaces Overview	23
	Figure 1: Platform with Most Incidents Gadget	25
	Figure 2: Devices with Most Incidents Gadget	25
Part 3	Administration	
Chapter 10	Organizations	41
	Figure 3: Manage Organizations Page	42
	Figure 4: Add Member Dialog Box	46
	Figure 5: Test Connection Dialog Box	49
	Figure 6: Messages Assigned to Connected Member Page	50
Chapter 12	Service Now Devices	55
	Figure 7: Service Now Devices Page	56
	Figure 8: Select Devices to Add to Service Now and Click Submit Page	58
	Figure 9: Install Event Profile Dialog Box	59
	Figure 10: Potential Exposure to Known Issues Page	61
	Figure 11: On-demand Incident Dialog Box	66
	Figure 12: Create On-demand Incident Status Dialog Box	67
	Figure 13: Add to Auto Submit Policy Page	69
Chapter 13	Event Profiles and AI-Scripts	71
	Figure 14: View Event Profiles Page	72
	Figure 15: Add Event Profile Page	75
	Figure 16: Potential Exposure to Known Issues Page	77
	Figure 17: Push to Devices Dialog Box	81
	Figure 18: Potential Exposure to Known Issues Page	82
	Figure 19: View Event Profiles Page	84
	Figure 20: Add Script Bundle Dialog Box	87
Chapter 14	Global Settings	91
	Figure 21: Global Settings Page	92
Chapter 15	Auto Submit Policy	99
	Figure 22: View Auto Submit Policy Page	100
	Figure 23: Auto Submit Policy Creation Page	101
	Figure 24: Choose Events to Include in Auto Submit Policy Page	102
Part 4	Service Central	
Chapter 16	Incidents	109

	Figure 25: Export JMB to HTML Dialog Box	114
	Figure 26: End-Customer Cases Dialog Box	120
Chapter 17	Information	121
	Figure 27: Choose Connected Members Dialog Box	125
	Figure 28: View JMB Dialog Box	128
Chapter 18	JMB Errors	129
	Figure 29: Download JMB Errors Dialog Box	129
Chapter 19	Notifications	131
	Figure 30: Create Notifications Page	133

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xii
Part 1	Overview	
Chapter 5	Service Now Modes	19
	Table 2: Tasks Enabled for Service Now Modes	20
Chapter 6	Service Now Dashboard and Workspaces Overview	23
	Table 3: Service Now Workspaces	24
Chapter 7	Service Now Icons	27
	Table 4: Inventory Page Icon Description	28
Chapter 8	User Roles	31
	Table 5: Predefined Service Now User Roles and Permissions	32
Part 3	Administration	
Chapter 10	Organizations	41
	Table 6: Organization Column Descriptions	42
	Table 7: Organization Credentials Page Field Descriptions	45
Chapter 12	Service Now Devices	55
	Table 8: Service Now Devices Column Descriptions	56
Chapter 13	Event Profiles and AI-Scripts	71
	Table 9: Add Event Profile Page Field Descriptions	75
Chapter 14	Global Settings	91
	Table 10: Global Settings Parameters	93
	Table 11: Global Settings Command Buttons	93
Chapter 15	Auto Submit Policy	99
	Table 12: Icons That Represent the Event Types and Their Descriptions	102
	Table 13: Auto Submit Policy Icons	105
Part 4	Service Central	
Chapter 19	Notifications	131
	Table 14: Notification Policies Table Column Descriptions	131
	Table 15: Create Notification Policy Page Field Descriptions	134

About the Documentation

- [Junos Space Documentation and Release Notes](#) on page xi
- [Documentation Conventions](#) on page xi
- [Documentation Feedback](#) on page xii
- [Requesting Technical Support](#) on page xii

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.

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

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

[Table 1](#) on [page xii](#) defines the 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.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/> . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [Service Now Overview on page 3](#)
- [Quick Start Guide to Service Now on page 7](#)
- [Upgrading Service Now on page 13](#)
- [Service Now MIBs on page 17](#)
- [Service Now Modes on page 19](#)
- [Service Now Dashboard and Workspaces Overview on page 23](#)
- [Service Now Icons on page 27](#)
- [User Roles on page 31](#)

CHAPTER 1

Service Now Overview

- [Service Now Overview on page 3](#)

Service Now Overview

Service Now is an application that helps automate fault management and accelerate issue resolution. It significantly reduces response time by automating support processes and uses device diagnostics for fault monitoring and case automation. Your contract with Juniper Networks determines whether Service Now operates in standard mode, end-customer mode, or offline mode. These modes in turn determine which tasks are enabled and disabled in Service Now. See "[Service Now Modes](#)" on page 19.

To help ensure maximum network uptime, AI-Scripts are installed on devices, which then automatically detect and report incidents to Service Now. When an event such as a process crash, an application-specific integrated circuit (ASIC) error, or a fan failure is detected in devices with AI-Scripts enabled, AI-Scripts automatically collect diagnostic data and packages it into a file called a *Juniper Message Bundle* (JMB). JMBs contain comprehensive information about the device identity, the problem event, and diagnostics. This information is securely transferred to the Junos Space platform. Service Now then notifies users of the new incident by sending an e-mail or an SNMP trap. In addition to reporting incidents, AI-Scripts also collect device information regularly in the form of *Information Juniper Message Bundles* (iJMBs). In Service Now, JMB errors are JMBs that do not comply with the standard data structure that is expected by Service Now or that contain unexpected data elements. Service Now identifies these JMBs and displays them on the Manage JMB Errors page, where they can be viewed and downloaded.



NOTE: Service Now uses the loopback interface on the device to collect JMBs whenever an event occurs. A device running Junos OS might have trouble sending JMBs to Service Now if the device does not allow traffic to the local host address (127.0.0.1).

You (the administrator) can fix this by adding the following firewall rule to the device:

```
set firewall family inet filter scp-block term ais-scp from
source-address 127.0.0.1/32
set firewall family inet filter scp-block term ais-scp from
destination-address 127.0.0.1/32
set firewall family inet filter scp-block term ais-scp from protocol
tcp
set firewall family inet filter scp-block term ais-scp from port 22
set firewall family inet filter scp-block term ais-scp then accept
```

```
Router001# show firewall family inet filter scp-block term ais-scp
from {
source-address {
127.0.0.1/32;
}
destination-address {
127.0.0.1/32;
}
protocol tcp;
port 22;
}
then accept;
```

If you do not want to use the loopback address, you can modify the configuration to use the device management IP address instead of the loopback address to collect JMBs.

After reviewing information provided in the JMB, you can submit the incidents to Juniper Support Systems (JSS) to create a Juniper Networks Technical Assistance Center (JTAC) case. The case is processed and analyzed to provide faster analysis and alerts. Using Service Now, you can track the status of the case. To restrict the amount of information you share with Juniper Networks, you can filter configuration content from iJMBs before submission.

Apart from submitting JMBs to obtain resolutions, you can use Service Now to perform tasks such as assigning an owner (user), flagging users to keep them notified of changes that are made, updating incident status, and deleting JMBs from the Service Now database. The data in incidents and information messages can also be exported into different file formats such as HTML, CSV, and Excel, and saved on the local file system. set up notification policies users who need to be kept informed of changes that affect them.

To add multiple devices and organizations, you need to obtain a technical support contract with the right level of service. After you have a valid contract, you can submit incidents and iJMBs to JSS for support. Without a valid contract, Service Now runs in demo mode

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

To open technical support cases and share iJMBs with Juniper Networks, you must first set up 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. After creating an organization, you can test its connectivity with JSS and even set the submission of incidents as test cases. 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.

You can group network elements and manage multiple devices as a single entity using Service Now device groups. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. Device groups help you regulate access to Service Now devices. After you add devices and create device groups, you can perform various operations on them, such as installing or removing AI-Scripts individually on every device or on all the devices in a device group simultaneously. You can even edit their parameters and delete them from the Service Now database.

In addition to monitoring and managing devices, organizations, and device groups, you can incorporate the use of SNMP and proxy servers. SNMP servers act as destinations where traps are sent when a notification policy is triggered. Configuring Service Now to work with a proxy server facilitates all communication to and from JSS through the proxy server, ensuring secure transactions.

The Service Now dashboard displays the gadgets and the workspaces that the user can use to perform various tasks. For more information about the Service Now dashboard and icons, see [“Service Now Dashboard Overview” on page 23](#).

To install, upgrade, and remove Service Now, you need Junos Space administrator privileges. Adding a Junos Space Application and Uninstalling a Junos Space Application in the *Network Application Platform User Guide* at http://www.juniper.net/techpubs/en_US/junos-space2.0/information-products/topic-collections/junos-space-network-application-platform-pwp/junos-space-network-application-platform-pwp.pdf. You can install, remove, or upgrade Service Now even while Junos Space and Junos Space applications are still running.

With different Service Now user privileges, you can perform one or more of the following tasks:

- Add devices to Service Now from the Junos Space platform.
- Add or delete a script bundle.
- Install or remove AI-Scripts on devices.
- Add, modify, or delete devices and device groups.
- Associate devices with device groups.
- Add, modify, or delete an organization.

- Submit incidents as test cases.
- Test organization connectivity to JSS.
- Export device data in CSV and Excel formats.
- View information about devices that risk the chance of exposure.
- Export inventory information in CSV and Excel formats.
- Configure the global settings (SNMP server and proxy server settings).
- Assign an owner, flag to users, update status of incidents, and delete incidents.
- View and delete iJMBs, and export device data into HTML format.
- Assign an owner, notify users, and delete an information message.
- View, download, and delete JMBs with errors.
- Create, edit, and delete a notification policy.

**Related
Documentation**

- [Service Central Overview on page 107](#)
- [Administration Overview on page 39](#)

CHAPTER 2

Quick Start Guide to Service Now

- [Service Now Quick Start on page 7](#)

Service Now Quick Start

- [Downloading the Junos Space VM image on page 7](#)
- [Setting Up Junos Space on page 8](#)
- [Setting Up Service Now in Standard Mode on page 9](#)
- [Setting Up Service Now in partner-proxy Mode on page 10](#)

Downloading the Junos Space VM image

System Requirements

You can use the VMWare OVF Tool to deploy one or more Junos Space virtual appliances to a VMware ESX or ESXi host server.

The Junos Space Virtual Appliance requires a VMware ESX server, version 3.5 or later, or a VMware ESXi server, version 4.0 or later, that can support a virtual machine with the following configuration:

- 64-bit quad processor with at least 2.66 GHz
- 8 GB memory
- One RJ-45 10/100/1000 Network Interface Card
- 45 GB hard disk (5 GB initial disk resources + 40 GB disk resources to be added)

You can download the Junos Space VM Image from <http://www.juniper.net/support/products/space/#sw>. The VM is delivered as an Open Virtualization Format (.ovf) file.

Download the installation package for the VMware ESX server from <http://www.vmware.com/download/vi/>.

To view installation instructions for the VMware ESX server, go to http://www.vmware.com/support/pubs/vi_pubs.html.

Setting Up Junos Space

After you have loaded Junos Space on the VM server and have powered on the Junos Space Virtual Appliance, select the Console tab, and log in using the default username (admin) and password (abc123).

After you log in to the CLI, configure the following settings:

1. Enter a new IP address for interface eth0.
2. Enter the default gateway as a dotted-decimal IP address.
3. Enter the nameserver address in dotted-decimal notation.
4. Configure a separate interface for device management. (This step is needed only if the devices running Junos OS are not reachable on interface eth0.)
5. If you do not want to add the appliance to an existing node cluster, or if the appliance is the first node in the cluster, enter **n** when you are prompted **Will this Junos Space system be added to an existing cluster?**
6. Enter an IP address for the Web GUI. Ensure that the address is on the same subnet as eth0.
7. Add an NTP server.
8. Enter a display name for the node.
9. Enter the password for the cluster maintenance mode. The maintenance mode administrator specifies this password, used to access maintenance mode and shut down all nodes.
10. A summary of the configured settings appears. If these settings are correct, type **A** to apply them.

After Junos Space has completed applying the settings, you are ready to configure the Service Now application on the Junos Space platform through the Web GUI.

Setting Up Service Now in Standard Mode

After you have completed the initial Junos Space configurations, you can configure Service Now through the Web GUI.

To set up Service Now in the standard mode:

1. **Log in to the Junos Space Web GUI**

Open an Internet browser and enter **https://xxx.xxx.xxx.xxx/mainui/**, where xxx.xxx.xxx.xxx is the IP address that you specified in Step 8 of “[Step-by-Step Procedure](#)” on page 8

Log in using the default username (super) and password (juniper123).

For more information, see [Administration Overview](#).

2. **Review the global settings in Service Now > Administration > Global Settings.**

- Set the interval to scan devices for informational Juniper Message Bundles (iJMBs).
- Set the SMTP server (IP address or hostname).
- Verify the connection status of Service Now to Juniper Support Systems (JSS) or Service Now to the partner-proxy (from end-customer mode).

For more information, see [Configuring Global Settings](#).

3. **Create an organization in Service Now > Administration > Organizations.**

Create an organization that represents a unique Juniper Networks CSS user and site ID. For more information, see [Adding an Organization](#).

4. **Create a device group.**

Create a device group that groups similar devices within an organization. For more information, see [Creating a Device Group](#).

5. **Add Devices to Junos Space.**

This is a three-step process that consists of discovering targets, specifying probes, and specifying credentials.

For more information, see [Discovering Devices](#).

**NOTE:**

You can add a device using device discovery under the following conditions:

- The device is configured with a static management IP address that is reachable from the Junos Space server.
- A user with full administrative privileges is created on the device for the Junos Space administrator.
- If you plan to use SNMP to probe devices as part of device discovery, SNMP is enabled on the device with appropriate read-only V1/V2C/V3 credentials.

6. Install Scripts.

Use Service Now to install an event profile on the devices running Junos OS. For more information, see [Installing an Event Profile on Devices Using Service Now](#).

Setting Up Service Now in partner-proxy Mode

After you have completed the initial Junos Space configurations, you can configure Service Now through the Web GUI.

To set up Service Now in the partner-proxy mode:

1. Log in to the Junos Space Web GUI

Open an Internet browser and enter **<https://xxx.xxx.xxx.xxx/mainui/>**, where xxx.xxx.xxx.xxx is the IP address that you specified in Step 8 of “[Step-by-Step Procedure](#)” on page 8

Log in using the default username (super) and password (juniper123).

For more information, see [Administration Overview](#).

2. Review the global settings in Service Now > Administration > Global Settings.

- Set the interval to scan devices for informational Juniper Message Bundles (iJMBs).
- Set the SMTP server (IP address or hostname).
- Verify the connection status of Service Now to the partner-proxy (from end-customer mode).

For more information, see [Configuring Global Settings](#).

3. Create an organization in Service Now > Administration > Organizations.

If you have an Advanced Service Contract, either Advanced Customer Support (ACS) or Advanced partner Support (APS), ensure that you have been allocated a separate site ID. If not, contact your Juniper Networks Service Manager to assist you with the discovery and allocation of site IDs.

Associate the site ID to an organization. For more information, see [Adding an Organization](#).

4. **Add a connected member.**

- a. After you (the partner) create an organization, generate and share the parameters (the IP address of the partner proxy, and the user name and password for the partner proxy organization) of the connected member with the end customer.
- b. After you have shared the connected member parameters, connect the connected member to the partner proxy.

As an end customer, you can set up Service Now in the End Customer Mode and enter the parameters needed to connect to the partner proxy.

For more information, see [Adding a Connected Member](#).

- c. At the customer site, you must activate the end-customer or connected-member mode by checking the **Connect to Another Junos Space** check box in the Global Settings page, entering the IP address or hostname of the partner-proxy, and clicking **Submit**.

5. **Associate Service Now devices to a device group.**

For more information, see [Associating Devices with a Device Group](#) and [Modifying a Device Group](#).



NOTE: Ensure that you first add the device running Junos OS to the Service Now application of the connected member, and send the iJMBs to the partner-proxy. Only then can the device appear in the partner-proxy device list.

Ensure that you follow a naming convention within the partner for organization names, connected members, and device groups.

6. **Review the notification policy.**

After you add new nodes, you must confirm that the required notification policies were added. For more information, see [Notification Policies Overview](#).

7. **Generate a test event.**

We recommend that new customers generate a test event to verify the process flow.

To generate a test event, load a script, which you can obtain from your Juniper Networks Service Automation contact, to the customer device to simulate the a real event capture. The test event is successful if the devices were correctly added to both the customer's and the partner's Service Now applications. You are notified if the test is successful.

CHAPTER 3

Upgrading Service Now

- [Upgrading Service Now on page 13](#)

Upgrading Service Now

You can upgrade Service Now to up to two versions later than its current version. For example, Service Now version 1.2 can be upgraded to versions 1.3 or 1.4. To upgrade from Service Now version 1.2 to a version later than 1.4, you must first upgrade to version 1.4 and then upgrade again to the required version.



NOTE: Service Insight is automatically upgraded along with Service Now.

You can upgrade Service Now and Service Insight in one of the following ways:

- **As part of the Platform upgrade:** When you upgrade the Junos Space Platform, Junos Space determines the running versions of the Service Now and Service Insight applications, and upgrades them to the latest versions. If the running versions are the latest, then Junos Space continues with the rest of the Platform upgrade without upgrading Service Now or Service Insight.

For information on upgrading the Platform, see “Upgrading the Network Application Platform” in the *Junos Space Network Application Platform User Guide*.

- **As a separate application:** You can upgrade Service Now and Service Insight together as a separate hot-pluggable application.

To upgrade Service Now and Service Insight together as a separate hot-pluggable application:

1. Ensure that the image to which you want to upgrade is downloaded to the local client file system using <https://www.juniper.net/support/products/space/#sw>.
2. Click **Platform > Administration > Manage Applications**.
The Manage Applications inventory page appears.
3. Select the **Service Now** icon, and click **Upgrade Service Now** from either the **Actions** drawer or the right-click menu.

The Upgrade Service Now appears and displays all previously uploaded versions of the applications.

4. Do one of the following:

- If the application that you want to upgrade is listed in the Upgrade Application dialog box, select the file, and click **Upgrade**.

The application upgrade process begins. (Go to 5.)

- If the application that you want to upgrade is not listed in the Upgrade Application dialog box, click **Upload**.

The Software File page appears. For information on how to upload the application, go to 1.

5. You enter maintenance mode. Junos Space prompts you to enter a username and password to enter maintenance mode. The username is **maintenance**; the password is one that the administrator created during the initial installation process.

6. Enter the maintenance mode username and password in the text field.

7. Click **OK**.

Junos Space displays a status window during the upgrade process.

8. When the Service Now upgrade finishes, a message appears confirming that Service Now was successfully deployed.



NOTE: The upgrade process takes between 2 and 30 minutes to finish depending on the size of the Junos Space database.

To upload a new application:

1. Select one of the following options:

- Click **Upload via HTTP**.

The **Software File** dialog box appears. Enter the application name, or click **Browse** to navigate to the new Junos Space application file on the local file system, and then click **Upload**.

- Click **Upload via SCP**.

The **Upload Software via SCP** dialog box appears. Enter the requested credentials: username, password, host IP address, and local pathname of the Junos OS application file. Click **Upload**.

The new applications are uploaded from the local file system into Junos Space and displayed by application name, filename, version, release level, and required version. When the process is completed the **Upgrade Job Information** dialog box appears.

2. In the **Upgrade Job Information** dialog box, click the Job ID link to see the Upgrade Application job on the Manage Jobs inventory page.

3. Click **Administration > Manage Applications** to continue with the add application process.

The Manage Applications inventory page appears.

4. Right-click the **Service Now** application and select **Upgrade Service Now**.
5. Click **OK**.

The **Upgrade Service Now** dialog box appears. You see the application file that was uploaded.

6. Select the application file to which you want to upgrade, and click **Upgrade**. The application upgrade process begins.

When you upgrade an instance of Service Now that operates in the end-customer or partner-proxy mode, ensure that the Service Now is either the same version or no more than two versions later than the end-customer Service Now applications that it connects to.

For example, as a Service Now end-customer, if you upgrade to Service Now 1.3, the Service Now that you connect to should be upgraded to Service Now version 1.3, 1.4, or 2.0. A Service Now upgraded to Service Now version 2.0 can only connect to end-customer Service Now application versions 2.0, 1.4, and 1.3.

**Related
Documentation**

- [Upgrading Junos Space Software](#)

CHAPTER 4

Service Now MIBs

- [Service Now MIBs on page 17](#)

Service Now MIBs

Service Now supports Juniper Networks enterprise-specific management information bases (MIBs). These MIBs define the traps that Service Now sends to a remote network management system. The sent traps correspond to the trigger specified for a reaction policy. For more information about creating a reaction policy in Service Now, see [“Creating and Editing a Notification Policy” on page 132](#).

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

To download the MIB files, navigate to the Service Now home page and click the **click here** link within the **Notices** dialog box. In order to monitor the devices with SNMP using an MIB browser (or other SNMP trap receivers such as HP OpenView), you must ensure that the following MIB files are loaded. Load the jnx-smi.mib file first.

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

- Related Documentation**
- [Adding an SNMP Server on page 94](#)
 - [Service Now Overview on page 3](#)

CHAPTER 5

Service Now Modes

- [Service Now Modes on page 19](#)

Service Now Modes

- [Overview on page 19](#)
- [Activating Offline, End-Customer and Partner-Proxy Modes on page 21](#)

Overview

Depending on your contract with Juniper Networks, Service Now operates in standard, end-customer, and partner-proxy modes. Service Now enables and disables certain features based on its mode of operation. The modes in which Service Now operates are:

- **Demo mode**—Service Now operates in demo mode until you create a Service Now organization and validate the organization's connection with JSS. In demo mode, Service Now supports a single organization and up to five devices. The connection between Service Now and Juniper Support Services (JSS) is disabled, preventing the creation of technical support cases.
- **Offline mode**—You can accept a standalone or partner-proxy license file and activate the Junos Space Platform and Service Now application without having to connect to the Juniper Support Service (JSS). You can perform all Service Now tasks except submit cases, create auto submit policies, view exposure, or view cases in Case Manager. You do not have the option to work in offline mode if Service Now is already in the end-customer mode.
- **Standard mode**—In standard mode, you can add multiple Service Now organizations and devices. Service Now is connected to JSS which enables JSS to provide support for the incidents and device snapshots that you submit.
- **End-customer mode**—In Service Now end-customer mode, Service Now and JSS communicate through the partner's Service Now application. A partner manages multiple end-customers using a secure HTTPS connection that is established between the end-customer and partner's Service Now applications.

Standard mode and end-customer mode have similar functions; however, end-customer mode allows the user to create only one organization. When an end-customer uses the credentials sent by the partner to create an organization, and the organization's connection with JSS is validated, a unique ID is assigned to the end-customer.

To connect to the partner, an end-customer must specify the partner's IP address or domain in the Service Now Global Settings page. While incidents are submitted to JSS in the standard mode, in end-customer mode you submit incidents to the Service Now partner, who in turn sends case updates back to the end-customer. The partner can also submit cases to JSS on behalf of the end-customer.

- **Partner-proxy mode**— If you are a qualified Juniper Networks partner, you can use Service Now in partner-proxy mode to manage multiple end-customer Service Now applications. A secure HTTPS connection is made between the Service Now applications of every end-customer and the partner, as well as between the partner and JSS. The Service Now partner receives JMBs from several end-customers and can submit JMBs to JSS on behalf of the end-customer or handle the cases without JSS support.

In this mode, you can add multiple organizations and devices groups. You associate every end-customer with an organization. Cases created by end-customers are opened with Juniper Networks under the site ID used for this associated organization. When you add a connected member, a default device group is created. You cannot delete this device group manually; however, it is automatically deleted when the connected member is deleted.

To connect to an end-customer, a Service Now partner uses a self-signed security certificate. Although this method of identification is not trusted, this certificate is automatically accepted to ensure that the communication between the partner and the end-customer is encrypted.

Table 2 on page 20 lists the tasks that are enabled for the Service Now modes.

Table 2: Tasks Enabled for Service Now Modes

Task	Demo Mode	Standard Mode	End-Customer Mode	partner-proxy Mode
Adding more than five devices	–	Enabled	Enabled	Enabled
Adding more than one organization	–	Enabled	–	Enabled
Adding connected members	–	–	–	Enabled
Updating end-customer cases	–	–	–	Enabled
Assigning messages to an end-customer	–	–	–	Enabled
Viewing messages assigned to an end-customer	–	–	–	Enabled
Creating technical Support Cases	–	–	–	Enabled

Table 2: Tasks Enabled for Service Now Modes (*continued*)

Task	Demo Mode	Standard Mode	End-Customer Mode	partner-proxy Mode
Installing and removing AI-Scripts on devices	Enabled	Enabled	Enabled	Enabled (only for partner's devices)
Other tasks	Enabled	Enabled	Enabled	Enabled

Activating Offline, End-Customer and Partner-Proxy Modes

Offline Mode:

To activate offline mode:

1. Obtain the standalone or partner-proxy license file from Juniper Networks.
2. In the Global Settings page, select **Offline Mode**, and click **Browse** to open the File Upload window. Select the license file and click **Upload**. For more information, see [“Configuring Global Settings” on page 91](#).
3. Add an organization by entering the name of the organization and the JMB filter level. For more information, see [“Adding an Organization” on page 43](#).

Offline mode is activated.



NOTE: Service Insight is disabled when Service Now is in offline mode.



NOTE: You must ensure that the version of the Junos Space Service Now application matches the version of the license you upload.

You can move Service Now from offline to online mode by selecting the **Online** option in the Global Settings page. To move from offline to online mode, you need to first create or modify the organization using partner credentials. This enables you to select the **Online** option in the Global Settings page, activate the Online Partner mode, and connect to JSS using a valid organization with a partner license.

End-Customer Mode:

To activate end-customer mode:

1. Obtain the organization credentials from the Service Now partner.
2. In the Global Settings page, select **End-Customer** and select the **Connect to Another Junos Space** check box, enter the IP address or hostname of the partner, and click **Submit**. For more information, see [“Configuring Global Settings” on page 91](#).
3. Add an organization using the credentials provided by the partner. For more information, see [“Adding an Organization” on page 43](#).

End-customer mode is activated.

Partner-Proxy Mode:

To activate the partner-proxy mode:

1. From the Manage Organizations page in Service Now, add an organization using the credentials provided with the Service Now license. For more information, see [“Adding an Organization” on page 43](#).

This activates the partner-proxy mode, which enables you to add end-customers and perform tasks that are exclusive to partner-proxy mode.

2. Add connected members to Service Now. For more information, see [“Adding a Connected Member” on page 46](#).

This enables you to manage multiple end-customer Service Now applications.

3. Send the username and password that you specified in step 1 to the end-customer. The end-customer uses the username and password to create an organization.

**Related
Documentation**

- [Administration Overview on page 39](#)
- [Service Central Overview on page 107](#)
- [Configuring Global Settings on page 91](#)
- [Adding an Organization on page 43](#)
- [Adding a Connected Member on page 46](#)

CHAPTER 6

Service Now Dashboard and Workspaces Overview

- [Service Now Dashboard Overview on page 23](#)

Service Now Dashboard Overview

The Service Now dashboard displays notifications and graphs about platforms and devices with most incidents. You can get to the Service Now dashboard in one of the following ways:

- Click **Service Now** from the Junos Space home page.
- Select **Service Now** from the Application Chooser.
- Select **Home** from any page within the Service Now workspaces.



The Service Now dashboard includes:

- [Service Now Workspaces on page 23](#)
- [Dashboard Gadgets on page 24](#)

Service Now Workspaces

Apart from the Service Central and Administration workspaces, Service Now also provides shortcuts to the Devices and Jobs workspaces by including them in the Service Now taskbar. [Table 3 on page 24](#) lists the tasks that can be performed using the Service Now workspaces.

Table 3: Service Now Workspaces

Workspace Icons	Workspace Name	Tasks
	Service Central	<ul style="list-style-type: none"> • Assign an incident owner, notify users of an incident, update the status of incidents, and delete incidents. • View and delete iJMBs, and export device data into HTML format. • Assign messages to end-customers (enabled if you are a Service Now partner). • Update end-customer cases (enabled if you are a Service Now partner). • View, download, and delete JMBs with errors. • View Knowledge Base (KB) articles associated with incidents. • View information about devices that risk the chance of exposure. • Assign an owner, flag to users, and delete an information message. • Create, edit, and delete a notification policy.
	Administration	<ul style="list-style-type: none"> • Add devices to Service Now from the Junos Space platform. • Add or delete an event profile or a script bundle. • Add and delete devices and device groups. • Install or remove AI-Scripts on devices. • Associate devices with device groups. • Add, modify, or delete an organization. • Add connected members and view messages assigned to them (enabled if you are a Service Now partner). • Run organizations in test mode and test organization connectivity to JSS. • Export device data in CSV and Excel formats. • Export inventory information in CSV format. • Configure the global settings (SNMP server and proxy server settings).

Dashboard Gadgets

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

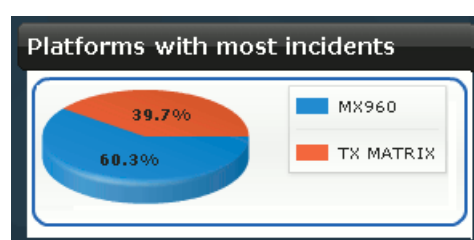
- [Platforms with Most Incidents on page 25](#)
- [Devices with the Most Incidents on page 25](#)
- [Service Now Notices \(Upgrade and Contract Notice\) on page 25](#)

Platforms with Most Incidents

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

For example, when you click the **MX960** element in the **Platforms with most incidents** gadget (as shown in [Figure 1 on page 25](#)), the Manage Incidents page displays only those incidents that were detected on the MX960 router.

Figure 1: Platform with Most Incidents Gadget

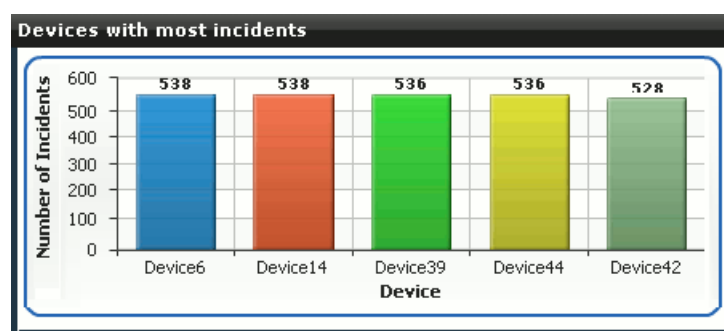


Devices with the Most Incidents

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

As shown in [Figure 2 on page 25](#), clicking **Device 6**, which is represented by the blue bar of the graph, displays the Manage Incidents page where incidents are filtered to display only those incidents that occurred on Device 6.

Figure 2: Devices with Most Incidents Gadget



Service Now Notices (Upgrade and Contract Notice)

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

- Related Documentation**
- [Service Central Overview on page 107](#)
 - [Administration Overview on page 39](#)
 - [Service Now Icons on page 27](#)

CHAPTER 7

Service Now Icons

- [Service Now Icons on page 27](#)

Service Now Icons

You can identify and differentiate various objects in the inventory pages of Service Now with the help of icons. These icons are displayed only in the thumbnail view of the inventory pages.

[Table 4 on page 28](#) lists and describes the Service Now inventory page icons.

Table 4: Inventory Page Icon Description




















Icons Displayed on the Inventory Page (Thumbnail View)	Icon Description	Icon Add-Ons	Description
Incidents			
	The incident occurred due to a software failure. It has medium priority.		Priority of the incident is critical.
	The incident occurred due to a hardware failure. It has medium priority.	 	Priority of the incident is high. Priority of the incident is medium
	The incident occurred due to resource exhaustion. It has medium priority.		Priority of the incident is low
	The incident occurred due to a general defect.	    	Incident case has been created. Incident case creation failed. Incident status is updated. End-customer incident that is updated. End-customer incident that is closed.
View Tech Support cases			
	Technical support case		The case is the technical support case of a connected member.
Information			
	Device snapshot		Device snapshot upload to JSS is successful.
			Device snapshot submission failed.
JMB Errors			
	JMB status: Error		

Table 4: Inventory Page Icon Description (*continued*)



















Icons Displayed on the Inventory Page (Thumbnail View)	Icon Description	Icon Add-Ons	Description
Incidents			
	JMB status: Invalid		
Notifications			
	Notification policy		A notification is sent when an incident is detected.
			A notification is sent when an incident is submitted.
			A notification is sent when a case id is assigned.
			A notification is sent when the case status is updated.
			A notification is sent when a new intelligence update is received
			The status of the reaction policy is enabled.
			The status of the reaction policy is disabled.
Organization			
	Licensed Service Now organization.		Service Now connected member or end-customer.
			Unlicensed Service Now organization.
Device Groups			
	Service Now device group		Device group of a Service Now connected member
Service Now Devices			

Table 4: Inventory Page Icon Description (*continued*)

Icons Displayed on the Inventory Page (Thumbnail View)	Icon Description	Icon Add-Ons	Description
Incidents			
	Service Now licensed device that has no issues and does not have scripts installed.		Device has AI-Scripts installed.
			Device has the following issues <ul style="list-style-type: none"> • No JMBs ever sent to Service Now • Stopped sending JMBs for over two weeks. • Connection failure
			Device has been exposed to known issues.

- Related Documentation**
- [Service Now Dashboard Overview on page 23](#)
 - [Service Now Overview on page 3](#)

CHAPTER 8

User Roles

- [Service Now User Roles on page 31](#)

Service Now User Roles

The Junos Space User Administrator creates users and assigns roles (permissions) that allow you to access and perform different tasks. You cannot view the tasks that you do not have access to. While Junos Space enables you to create users with custom permissions, it also has a set of predefined user roles. You cannot modify or delete these predefined roles. See [Table 5 on page 32](#), which describes the tasks that predefined Service Now users have access to, based on the roles assigned to them.

You can create users and manage them on the Manage Users page, if you have User Administrator permissions.

To create and manage these users, select **Application Switcher > Network Application Platform > Users > Manage Users**. The Manage Users page lists the existing users. Use this page to create and assign roles to Service Now users.

You can also navigate to the Manage Users page by selecting **Application Switcher > Jump to Users**.

Table 5: Predefined Service Now User Roles and Permissions

Role	Permitted to Execute Actions Under the Following Subtasks	
Service Now Admin	Administration	Service Now Devices, New Device Platform Event Profiles, Add Event Profile Script Bundle, Add Script Bundle Organization, Add Organization Global Settings, SNMP Configuration, Proxy Server Configuration Device Group, Create Device Group View Auto Submit Policy, Create Auto Submit Policy
	Service Central	Incidents, View Tech Support Cases JMB Errors Information, Messages, Device Snapshots Notifications, Create Notification
Service Now Unrestricted User	Administration	Service Now Devices
	Service Central	Incidents, View Tech Support Cases JMB Errors Information, Messages, Device Snapshots Notifications, Create Notification Permissions exclude the ability to delete managed objects
Service Now Read Only User	Administration	Viewing and exporting Service Now devices
	Service Central	Viewing JMB details Exporting incident summary into an Excel format Viewing an incident case in the Case Manager Viewing a technical support case in Case Manager View end-customer cases in Case Manager Downloading JMB errors Scanning an information message for impact Exporting a JMB (device snapshot) to HTML Viewing JMB (device snapshot) details Viewing notification policies

You can flag or assign an incident only to a Service Now Admin or Service Now Unrestricted User. You can flag or assign an information message or iJMB to any user. Regardless of the permissions you have, you can always clear a flag of an incident or information message that had been flagged to you.

- Related Documentation**
- [Service Central Overview on page 107](#)
 - [Administration Overview on page 39](#)

PART 2

Using the Service Now Getting Started Assistant

- [Service Now Getting Started Assistant Usage Overview on page 37](#)

CHAPTER 9

Service Now Getting Started Assistant Usage Overview

Service Now Getting Started Assistant Usage Overview

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

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

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

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

The following steps are required:

1. Review Global Settings.
See [“Configuring Global Settings” on page 91](#)
2. Create Organization.
See [“Adding an Organization” on page 43](#).
3. Add Devices to Junos Space.
See the *Discovering Devices* section from the *Network Application Platform User Guide*.
4. Create Device Group.
See [“Creating a Device Group” on page 51](#).
5. Install Scripts using Service Now Devices.
See [“Installing an Event Profile on Devices Using Service Now” on page 59](#)

The following step is optional:

- Add New Script Bundle.
See [“Adding a Script Bundle to Service Now” on page 87](#).

To activate Service Now in end-customer and partner-proxy modes, see the Activating the End-Customer and Partner-Proxy Modes section in [“Service Now Modes” on page 19](#).

**Related
Documentation**

- [Service Now Overview on page 3](#)

PART 3

Administration

- [Administration Overview on page 39](#)
- [Organizations on page 41](#)
- [Device Groups on page 51](#)
- [Service Now Devices on page 55](#)
- [Event Profiles and AI-Scripts on page 71](#)
- [Global Settings on page 91](#)
- [Auto Submit Policy on page 99](#)

Administration Overview

You can use Service Now to monitor and manage device data with the help of AI-Scripts that are installed on a device. When AI-Scripts are installed on a device, the device is considered AIS-enabled and can automatically detect and report incidents and informational JMBs (iJMBs).

AIS-enabled devices periodically send device data in the form of Informational Juniper Message Bundles (iJMBs) to Service Now. Using Service Now, you can add and manage devices, upload AI-Scripts bundles, and install the AI-Scripts on the devices.

You can also add devices that are part of the Junos Space platform to Service Now and group them under organizations. An organization is defined by a unique site ID that acts as a customer record in Juniper Networks CRM systems. After creating an organization, you can test its connectivity with JSS and even run it in test mode. Juniper Support Systems (JSS) provides support for the incidents and iJMBs that you submit. This support depends on your service contract level, such as J-Care Efficiency, Continuity, or Agility levels of service.

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. Service Now organizations are defined by the site ID (used when opening support cases) under devices and users.

By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes and control a user's access to devices. Device groups also help you automatically install AI-Scripts on many devices at one time.

Some administration tasks, such as adding connected members and viewing messages assigned to them, are enabled only when Service Now mode is activated. For more information about Service Now modes, see [“Service Now Modes” on page 19](#).

The Administration workspace enables you to perform the following tasks:

- Add devices to Service Now from the Junos Space platform.
- Add or delete an event profile or a script bundle.
- Add and delete devices and device groups.
- Install or remove AI-Scripts on devices.
- Associate devices with device groups.
- Add, modify, or delete an organization.
- Add connected members and view messages assigned to them (enabled if you are a Service Now partner).
- Run organizations in test mode and test organization connectivity to JSS.
- Export device data in CSV and Excel formats.
- Export inventory information in CSV Format
- Configure the global settings (SNMP server and proxy server settings).

**Related
Documentation**

- [Service Now Overview on page 3](#)
- [Service Now Modes on page 19](#)
- [Organizations Overview on page 41](#)
- [Device Groups Overview on page 51](#)
- [Service Now Devices Overview on page 55](#)
- [Event Profiles Overview on page 71](#)
- [AI-Scripts Overview on page 85](#)
- [Auto Submit Policy Overview on page 99](#)
- [Configuring Global Settings on page 91](#)

CHAPTER 10

Organizations

- [Organizations Overview on page 41](#)
- [Adding an Organization on page 43](#)
- [Adding a Connected Member on page 46](#)
- [Modifying Organization Parameters on page 47](#)
- [Deleting an Organization on page 48](#)
- [Test the Connection to JSS on page 48](#)
- [Viewing Messages Assigned to a Connected Member on page 49](#)
- [Running an Organization in Test Mode on page 50](#)

Organizations Overview

An organization in Service Now represents a unique Clarify site ID in Juniper Support Systems (JSS). JSS uses Clarify Site IDs to identify customers when providing technical support. You can manage multiple sites (each with its own Clarify site ID) using multiple organizations defined in Service Now with just one Service Now installation. This is done by dividing the network into multiple logical customer sites. To communicate with JSS, a Service Now organization requires a site ID, login name, and password. The login name must be a contact associated with the site ID.

Device groups are used to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. Using device groups, you can control the access that users have over devices. See [“Device Groups Overview” on page 51](#).

For more information about creating device groups, see [“Creating a Device Group” on page 51](#).

While you configure organizations to run Service Now in a preproduction environment, you can avoid the processing of production incident cases by running an organization in test mode. In this mode, the synopsis of the incident is appended with [Test] and JTAC recognizes the case as a test case and does not process it.

Service Now organizations are displayed on the Manage Organizations page. You can choose to display the organizations either as a table arranged according to name, site ID, submit cases as, username, and connection status, or as icons, as shown in [Figure 3 on page 42](#).

Figure 3: Manage Organizations Page

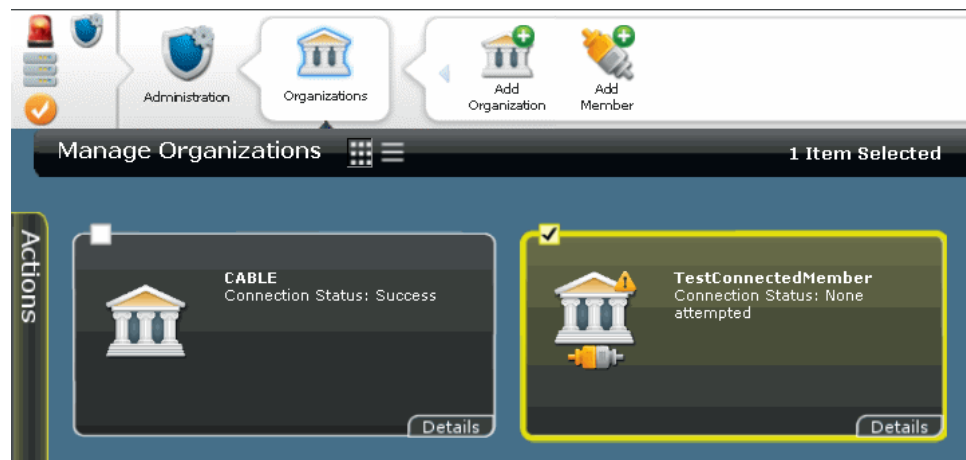


Table 6 on page 42 describes the fields displayed in the tabular view of the Manage Organizations page and in the **Organizations Details** dialog box.

Table 6: Organization Column Descriptions

Column Name	Description
Name	Name of the organization
Site ID	Identifier for the Customer Site in the JTAC Clarify system
Submit Cases As	Status of the case that is sent to JSS. It is a real case or a test case that is sent in a production environment. The synopsis of a test case sent to JSS is appended with [Test Mode]. When Service Now is in offline mode, this column is empty.
User Name	Name used to identify the user for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases You do not need to enter a user name or password if Service Now is in the offline mode.
Connection Status	Status of the connection between the organizations and JSS
JMB Filter Level (Only visible in the Detail Summary dialog box, which opens when you double-click the organization)	Amount of device configuration information in a JMB that can be shared with JSS

From the Organizations page, you can:

- Add an organization
- Add a member
- Modify organization parameters

- Run an organization in test mode
- Test connectivity to JSS
- Delete an organization

Related Documentation

- [Adding an Organization on page 43](#)
- [Adding a Connected Member on page 46](#)
- [Modifying Organization Parameters on page 47](#)
- [Deleting an Organization on page 48](#)
- [Test the Connection to JSS on page 48](#)
- [Viewing Messages Assigned to a Connected Member on page 49](#)
- [Running an Organization in Test Mode on page 50](#)

Adding an Organization

An organization in Service Now represents a unique Clarify site ID in Juniper Support Systems (JSS). Clarify Site IDs identify customers when JSS provides technical support. You can use multiple organizations defined in Service Now to manage multiple sites (each with its own Clarify site ID) with only one Service Now installation. This is done by dividing the network into multiple logical customer sites. To communicate with JSS, a Service Now organization requires a site ID, login name, and password. While creating an organization you can specify the amount of device configuration information in JMBs that you want to share with JSS, for devices associated with that organization.

To add a Service Now organization in partner mode:

1. From the Service Now taskbar, select **Administration > Organizations > Add Organization**.

The **Add Organization** dialog box appears.

2. Enter the organization parameters in the provided fields.
For a detailed description of these fields, see [Table 7 on page 45](#).



NOTE: In the offline mode, the Add Organization page displays only the **Name** and the **JMB Filter Level** fields.

3. Click **Submit**.

This action verifies and saves the organization parameters and returns to the Manage Organization page.

To add a Service Now organization in end-customer mode:

1. From the Service Now taskbar, select **Administration > Organizations > Add Organization**.

The **Add Organization** dialog box appears.

2. Enter the organization parameters in the provided fields.
For a detailed description of these fields, see [Table 7 on page 45](#).
3. Click **Submit**.

This action verifies and saves the organization parameters and returns to the Manage Organization page.



NOTE: In end-customer mode, you can add only one organization.

[Table 7 on page 45](#) defines the **Add Organization** dialog box fields.

Table 7: Organization Credentials Page Field Descriptions

Name	Description	Privileges	Range/Length	Default
Name	Name of the organization	Service Now administrator privileges	64 characters	Blank
Submit cases as	Status of the case that is sent to JSS. It is a real case or a test case that is sent in a production environment. The synopsis of a test case sent to JSS is appended with [Test Mode].	Service Now administrator privileges	The values are: <ul style="list-style-type: none"> Real cases Test cases 	Disabled
User Name	Name used to identify the user for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases You do not need to enter a user name or password if Service Now is in the offline mode.	Service Now administrator privileges	32 characters	Blank
User Password	Password used to log in for the account with the username you specify You do not need to enter a user name or password if Service Now is in the offline mode.	Service Now administrator privileges	32 characters	Blank
Get Sites (button)	Identifier for the Customer Site in the JTAC Clarify system Click Get Sites and select a Site ID from the Site ID list that is generated when you enter the username and password. NOTE: This option is not available when you add an organization in the end-customer mode.	Service Now administrator privileges	80 characters	Blank
JMB Filter Level	Amount of device configuration information in JMBs to be shared with JSS: <ul style="list-style-type: none"> Do not send—Sends no configuration information Send all information except configuration—Sends all device information except the configuration Send all information with IP Addresses overwritten—Sends all device information, except IP addresses Send all information—Sends all device information. Only send list of features used—Sends only the device configuration information 	Service Now administrator privileges	—	Do not send

- Related Documentation**
- [Organizations Overview on page 41](#)
 - [Running an Organization in Test Mode on page 50](#)

Adding a Connected Member

After you configure Service Now to run in partner-proxy mode, you can add multiple end-customers and manage end-customer Service Now applications over a secure HTTPS connection. The can communicate with the end-customer only after the Service Now application of an end-customer is activated. For more information about and end-customer modes, see “[Service Now Modes](#)” on page 19.



NOTE: You can add a connected member only after you create a valid organization.

To add a connected member to Service Now:

1. From the Service Now taskbar, select, **Administration > Organization > Add Connected Member**.

The **Add Member** dialog box appears as shown in [Figure 4 on page 46](#).

Figure 4: Add Member Dialog Box

A screenshot of the 'Add Member' dialog box. It has a dark blue header with the title 'Add Member'. The main area is a light blue rectangle containing five input fields: 'Name:', 'User Name:', 'User Password:', 'Confirm User Password:', and 'JMB Filter Level:'. The 'JMB Filter Level' field is a dropdown menu currently showing 'Do not send'. At the bottom of the dialog are two buttons: 'Submit' (blue) and 'Cancel' (red).

2. Enter a name for the connected member.
The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-).
3. Enter a username for the connected member.
The username must be in the format user@example.com.
4. Enter the password that can be used to log in with the username you have entered.
5. Enter the same password again to confirm.
6. Select one of the following values to specify the amount of device configuration information in a JMB that can be shared with JSS:

- Do not send—Sends no configuration information.
 - Send all information except configuration—Sends all device information except the configuration.
 - Send all information with IP Addresses overwritten—Sends all device information, except IP addresses
 - Send all information—Sends all device information.
 - Only send list of features used—Sends only the device configuration information.
7. Click **Submit**.

The connected member is created and displayed on the Manage Organizations page.

**Related
Documentation**

- [Adding an Organization on page 43](#)
- [Organizations Overview on page 41](#)

Modifying Organization Parameters

Using Service Now, you can modify the parameters of an organization.



NOTE: When you modify the parameters of a connected member, you cannot edit the name of the connected member and the organization associated with it. For more information about connected members see [“Service Now Modes” on page 19](#).

To modify the parameters of an organization:

1. From the Service Now taskbar, select **Administration > Organizations**.
The Manage Organizations page appears.
2. Select the organization whose parameters you want to modify.
3. Click **Modify Organization** from either the **Actions** drawer or the right-click menu.
The **Organizations** dialog box displays the name, submit cases as, username, and password, and the JMB filter level of the selected organization.
4. Make your changes to these parameters.
5. Click **Submit**.

The changes are saved in the Service Now database. To view these changes, view the details of the organization in the Manage Organizations page.

**Related
Documentation**

- [Organizations Overview on page 41](#)
- [Deleting an Organization on page 48](#)
- [Running an Organization in Test Mode on page 50](#)

Deleting an Organization

As a Service Now administrator, you can use the Service Now Manage Organizations page to delete organizations.



NOTE: You cannot delete an organization without first deleting its associated connected members.

To delete an organization:

1. From the Service Now taskbar, select **Administration > Organizations**.
The Manage Organizations page appears.
2. Select the organization that you want to delete.
3. Click **Delete Organization** from the **Actions** drawer or the right-click menu.
The **Delete Organizations** dialog box appears asking you to confirm the deletion.
4. Click **Delete**.

The selected organization is deleted from the Service Now database and no longer appears in the Manage Organizations page.



NOTE: When you delete an organization, you also automatically delete its associated device groups.

Related Documentation

- [Organizations Overview on page 41](#)
- [Adding an Organization on page 43](#)
- [Running an Organization in Test Mode on page 50](#)

Test the Connection to JSS

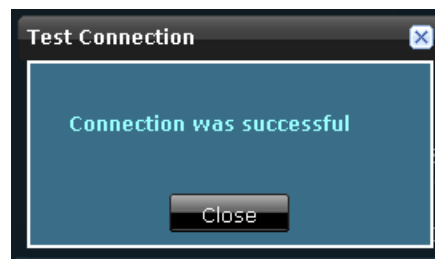
From the Manage Organizations page, you can test the connection of every organization with Juniper Support Systems (JSS).

To test an organization's connectivity with JSS:

1. From the Service Now taskbar, select **Administration > Organizations**.
The Manage Organizations page appears.
2. Select the organization whose connection to JSS you want to test.
3. Click **Check Status** from either the **Actions** drawer or the right-click menu.

The **Test Connection** dialog box displays the result of the test connection to JSS, as a success or a failure.

Figure 5: Test Connection Dialog Box



In case of a failure, a description appears stating the reason for the failure in connection.

4. Click **Close** to return to the Manage Organizations page.



NOTE: This option is not available when Service Now is in the offline mode.

Related Documentation

- [Organizations Overview on page 41](#)
- [Adding an Organization on page 43](#)
- [Deleting an Organization on page 48](#)
- [Running an Organization in Test Mode on page 50](#)

Viewing Messages Assigned to a Connected Member

Using Service Now, you can view the list of messages that are assigned to a connected member. This action is available only when Service Now operates in partner-proxy mode and when you select a connected member in the Manage Organizations page.

To view the messages assigned to a connected member:

1. From the Service Now taskbar, select **Administration > Organizations**.
The Manage Organizations page displays the list of organizations and connected members.
2. Select the connected member whose list of assigned messages you want to view.
3. Right-click your selection and select **View Messages** from either the **Actions** drawer or the right-click menu.

As shown in [Figure 6 on page 50](#), the Messages assigned to Connected Member page displays the list of messages assigned to the selected connected member.

Figure 6: Messages Assigned to Connected Member Page

Messages assigned to Connected Member		
Return to Organization		
Title ▲	Status	Sent
abc	Delivered	2010/05/07 01:36
final1	Delivered	2010/05/07 01:36

4. To view the details of the messages, click the title of the message.

The **Message Details** dialog box displays information such as the organization that the message is sent to, site ID, title, issue date, summary, instructions, keywords, relevance, owner, and the users that the message was flagged to.

5. Click **OK** to return to the Manage Organizations page.

Related Documentation

- [Assigning a Message to a Connected Member on page 124](#)
- [Messages Overview on page 121](#)
- [Adding a Connected Member on page 46](#)

Running an Organization in Test Mode

While configuring an organization, you can enable test mode so that you can submit cases as test cases and avoid the processing of production incident cases. In this mode, the synopsis of the incident that is being submitted to JTAC is appended with [Test].

To run an organization in test mode:

1. From the Service Now taskbar, select **Administration > Organizations**.

The Manage Organizations page appears.

2. Select the organizations that you want to place in test mode, and select **Modify Organization** from either the **Actions** drawer or the right-click menu.

The **Organization** dialog box displays the parameters of the selected organization.

3. Select **Test Cases** from the **Submit Cases as** list.
4. Click **Submit**.

This action ensures that incidents that are submitted to JSS are considered as test cases.

Related Documentation

- [Organizations Overview on page 41](#)
- [Modifying Organization Parameters on page 47](#)

CHAPTER 11

Device Groups

- [Device Groups Overview on page 51](#)
- [Creating a Device Group on page 51](#)
- [Modifying Device Groups on page 52](#)
- [Deleting Device Groups on page 53](#)

Device Groups Overview

You can use Service Now to group network elements and manage multiple devices in a single entity called a device group. You use device groups to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. You can associate one or more devices with every device group.

Only users with Service Now admin privileges can configure device groups.

From the Manage Device Groups page in Service Now, you can perform the following tasks:

- Creating and Adding Devices to a Device Group
- Modifying Device Groups
- Deleting Device Groups

Related Documentation

- [Creating a Device Group on page 51](#)
- [Modifying Device Groups on page 52](#)
- [Deleting Device Groups on page 53](#)

Creating a Device Group

You use device groups to group devices within an organization. Only users with Service Now admin privileges can create device groups and add devices to them.

To create a device group:

1. From the Service Now taskbar, select **Administration > Device Groups > Create Device Group**.

The Administration: Create Device Group page appears.

2. Enter a name for the device group within the **Name** field.
The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-).
3. In the **Organizations** list, select an organization for this device group.
If you want to add a new organization, click **New Organization**. See [“Adding an Organization” on page 43](#).
4. Select the devices that you want to add to this device group.
5. Click **Add**.

The selected devices are added to the device group. To verify that the devices have been added, you can view the details of the device group in the Manage Device Groups page.

- Related Documentation**
- [Device Groups Overview on page 51](#)
 - [Modifying Device Groups on page 52](#)

Modifying Device Groups

To modify a device group:

1. From the Service Now taskbar, select **Administration > Device Groups**.
The Manage Device Group page lists the existing device groups.
2. Select the device group whose parameters you want to modify, and select **Modify Device Group** from either the **Actions** drawer or the right-click menu.

The **Modify Device Group** dialog box displays the parameters of the selected device group.

3. Modify the fields as necessary.

Use the **Device Groups** navigation drawer on the right-hand corner of the screen to add or delete devices from the selected device group.

4. Click **Finish**.

The changes are submitted and new values are replaced in the Service Now database. The Manage Device Group page appears.

- Related Documentation**
- [Device Groups Overview on page 51](#)
 - [Deleting Device Groups on page 53](#)
 - [Creating a Device Group on page 51](#)

Deleting Device Groups

If you have Service Now admin privileges, you can delete device groups.

To delete a device group:

1. From the Service Now taskbar, select **Administration > Device Groups**.

The Manage Device Group page lists the existing device groups.

2. Select the device group that you want to delete, and select **Delete Device Group** from either the **Actions** drawer or the right-click menu.

The **Delete Device Group** dialog box prompts you to confirm the deletion.

3. Click **Delete**.

The selected device group is deleted from the Service Now database and no longer appears on the Manage Device Group page.

- Related Documentation**
- [Device Groups Overview on page 51](#)
 - [Modifying Device Groups on page 52](#)

CHAPTER 12

Service Now Devices

- [Service Now Devices Overview on page 55](#)
- [Adding Devices from the Platform on page 58](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)
- [Manually Installing AI-Scripts on Devices on page 62](#)
- [Uninstalling Event Profiles from Devices on page 63](#)
- [Exporting Device Data in CSV and Excel Format on page 63](#)
- [Exporting Inventory Information in CSV Format on page 64](#)
- [Viewing Exposure on page 64](#)
- [Generating On-Demand Incidents on page 65](#)
- [Deleting a Device on page 67](#)
- [Associating Devices with a Device Group on page 68](#)
- [Adding Devices to Auto Submit Policies on page 69](#)

Service Now Devices Overview

You can use Service Now to group network elements and manage multiple devices in a single entity called a device group. Service Now lists the devices that are already a part of the Junos Space platform and that you can import into Service Now. These devices periodically send device information to Service Now for monitoring purposes. Service Now also detects and displays devices that do not send device information (device snapshots) for more than 2 weeks.

After you add devices and create device groups, you can perform various operations on them, such as installing and removing AI-Scripts individually on every device or on all the devices in a device group simultaneously. You can also delete devices from the Service Now database.

Service Now devices are displayed on the Service Now Devices page. You can choose to display the devices either as a table arranged according to organization, device group, hostname, serial number, platform, version, and script bundle, or as icons as shown in [Figure 7 on page 56](#). [Table 8 on page 56](#) describes the columns in the Service Now Devices page and the **Device Detail** dialog box.

Figure 7: Service Now Devices Page

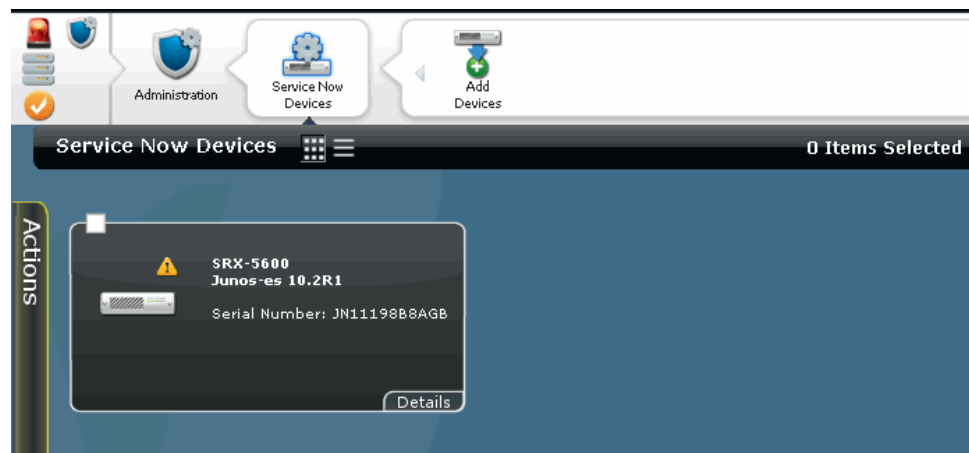


Table 8 on page 56 describes the fields displayed in the tabular view of the Service Now Devices page and in the **Device Details** dialog box.

Table 8: Service Now Devices Column Descriptions

Field Name	Description
Organization	Name of the organization to which this device belongs.
Connected Member	Name of the connected member.
Device Group	Name of the device group to which this device belongs.
HostName	Unique name by which the device is known on a network.
Serial Number	Serial number of device.
Product	Type of device
OS Version	Version of the Junos operating system that is running on the device.
Script Bundle	Name and version of the script bundle installed on the device.
Event Profile	Name and version of the event profile installed on the device.
Field displayed on the Details Summary Page	
Platform	Type of device (routing platform).
Routing Engine	Type of routing engine. The values are: <ul style="list-style-type: none"> • Single RE • Dual RE

Table 8: Service Now Devices Column Descriptions (*continued*)

Field Name	Description
Event Profile Installation Status	Status of event profile installation on the device. The values are: <ul style="list-style-type: none"> • Success • Failed • Master RE Failed • Backup RE Failed • Successfully installed in Master RE. Backup RE is inactive.
Connection Status	Status of connection from the device to Service Now.
Alerts	Status of iJMB upload.
Support Contract ID	A table that displays information about the support contract according to contract number, status, SKU, SKU type, as well as start and end dates. To get on-demand updates about your Service Now contract, click the Refresh button on the Device Details page.

From the Service Now Devices page you can perform the following tasks:

- Add devices from the platform
- Install event profiles on devices
- Remove event profiles from devices
- Export device data into CSV and Excel format
- Export inventory information in CSV format
- Associate devices with auto submit policies
- Delete devices
- View information about device that risk the chance of exposure to known issues
- Associate devices with a device group

Related Documentation

- [Adding Devices from the Platform on page 58](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)
- [Uninstalling Event Profiles from Devices on page 63](#)
- [Exporting Device Data in CSV and Excel Format on page 63](#)
- [Exporting Inventory Information in CSV Format on page 64](#)
- [Viewing Exposure on page 64](#)
- [Modifying Device Groups on page 52](#)
- [Deleting a Device on page 67](#)
- [Associating Devices with a Device Group on page 68](#)

Adding Devices from the Platform

You can add devices that are a part of the Junos Space platform to the Service Now application. While you add these devices, you can also assign them to a device group and also install AI-Scripts on them.



NOTE: Devices that are discovered and added to the Junos Space platform are automatically added to the Service Now application. However, if Service Now is in demo mode, only the first five devices are added.

To add devices from the Junos Space platform to Service Now:

1. From the Service Now taskbar, select **Administration > Service Now Devices > Add Devices**.

The Select Devices to Add to Service Now and Click Submit page displays the devices that have not been added to Service Now.

Figure 8: Select Devices to Add to Service Now and Click Submit Page

Host Name	Network Name	Serial Number	Product	Version
10.205.230.1	10.205.230.1	AD3009aa0006	SRK210-4M	10.292.10
10.205.230.6	10.205.230.6	AD3009aa0009	SRK210-4M	10.292.10
10.205.230.8	10.205.230.8	AD3009aa000e	SRK210-4M	10.292.10
10.205.230.2	10.205.230.2	AD3009aa000b	SRK210-4M	10.292.10
10.205.230.3	10.205.230.3	AD3009aa000c	SRK210-4M	10.292.10
10.205.230.100	10.205.230.100	AD3009aa0009	SRK210-4M	10.292.10
10.205.119.19	10.205.119.19	AT2510AF0924	SRK1008	11.282.4
10.205.119.19	10.205.119.19	AT2510AF0929	SRK1008	11.282.4
Node-177	10.205.50.177	AA3610AA0078	SRK3400	11.2.00110210.0
Node-178	10.205.50.178	AA3610AA0077	SRK3400	11.2.00110210.0
Corp-Gateway	10.205.119.2	A02610AA0089	SRK650	10.487.5

2. Select the devices that you want to add.
3. Click **Submit**.

The Add Service Now Device(s) page appears.

4. Click **Apply profiles to added devices (manually)** to go to the Install Event Profile page. For more information on installing profiles, see [“Installing an Event Profile on Devices Using Service Now” on page 59](#).

The devices are added to Service Now and displayed on the Service Now Devices page. The device **Status** column displays **Imported**.

Related Documentation

- [Service Now Devices Overview on page 55](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)
- [Adding Devices to Auto Submit Policies on page 69](#)

Installing an Event Profile on Devices Using Service Now

An event profile is a set of event scripts that are selected from an AI-Scripts bundle. When you install an event profile on Juniper Networks devices, the event scripts are installed on the devices and provide the information needed to automatically detect and report problem (incident) and information events, thus ensuring maximum network uptime.

Service Now uses Device Management Interface (DMI) to install and remove AI-Scripts on devices. DMI is an extension to the NETCONF network management protocol.

When you install event profiles on individual systems (chassis) with dual Routing Engines, Service Now installs the event profiles on both primary and backup Routing Engines.



NOTE: While operating in partner-proxy mode, you cannot install event profiles on a connected member's device.

To install an event profile on devices:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

2. Select the device on which you want to install the event profile.



NOTE: You can install event profiles on only those devices for which you can specify correct login credentials and that belong to a device group.

3. Click **Install Event Profile** from either the **Actions** drawer or the right-click menu.

The **Install Event Profile** dialog box appears as shown in [Figure 9 on page 59](#).

Figure 9: Install Event Profile Dialog Box

4. Select an event profile from the **Use Profile** procedure, which displays the event profiles that you upload into Service Now.
5. (Optional) If you do not want to save a copy of the event profile after it is installed on the device, select the **Never store Script Bundle files on device (if selected roll-back option will not be available)** check box.

6. (Optional) If you want to remove the script bundle from the device, after it is installed, select the **Remove Script Bundle files after successful install** check box.
7. (Optional) If you want to schedule a time for installation, select the **Schedule at a later time** check box, and specify the **Date and time** for the installation.
The installation process begins automatically at the time you specify.
8. Click **Submit**.
9. (Optional) If you want to add devices on which you want to install the selected event profile, select the **Install Event Profiles on new Devices** check box, and select the devices.
10. Click **Finish**.

The **Save Event Profile** dialog box appears.

11. Click one of the following links based on the required results.

Link	Result
Apply this profile to original set of devices	The Potential Exposure to Known Issues page displays information about the selected set of devices. A bang (!) icon is placed next to devices, associated with the event profile, that risk the chance of exposure.

Figure 10: Potential Exposure to Known Issues Page



- a. (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.
- b. (Optional) To view a device's exposure to known issues, click the respective link displayed in the **Exposure** column. The View Exposure page appears and displays the known issues associated with the respective device.
Click **Return to Potential Exposure** to continue.
- c. Click **Continue**.
A confirmation pop-up box procedures the final procedure of devices on which the selected event profile must be installed.
You can remove devices from the procedure by clearing the check boxes of the devices you want to delete.
- d. Click **Install**.
The selected event profile is installed on the devices with which it is associated, and the Service Now Devices page appears.
To view the status of the event profile installation task, click the job ID link and the Manage Jobs page displays the status of the job. Double-click the job to view information about each step of the installation.

Apply this profile to devices manually	<p>You are allowed to select Service Now devices on which you want to install the event profile. Select the devices and click OK. The Job Information dialog box displays the job ID. To view the status of the event profile installation task, click the job ID link and the Manage Jobs page displays the status of the job. Double-click the job to view information about each step of the installation.</p> <p>Click OK to return to the Manage Event Profiles page.</p>
Return to the Profiles Page	The event profile installation task is canceled, and the Manage Event Profiles page appears.

- Related Documentation**
- [Event Profiles Overview on page 71](#)
 - [AI-Scripts Overview on page 85](#)
 - [Manually Installing AI-Scripts on Devices on page 62](#)
 - [Adding a Script Bundle to Service Now on page 87](#)
 - [Viewing Exposure on page 64](#)

Manually Installing AI-Scripts on Devices

AI-Scripts can be installed on Junos OS devices manually using CLI mode. For manual installation of AI-Scripts on devices, you require the same login credentials that you use to discover devices in Junos Space.

To install AI-Scripts manually:

1. Copy the AI-Scripts install package (example: `jais-2.1R2.0-signed.tgz`) to the Junos OS device using SCP or FTP.
2. From configuration mode, execute the following commands:
`set groups juniper-ais system scripts commit allow-transients`
`set groups juniper-ais system scripts commit file jais-activate-scripts.slax optional`
`set groups juniper-ais event-options destinations juniper-aim archive-sites /var/tmp/`
3. Install the AI-Scripts bundle install package in CLI mode using the command **`request system scripts add <full-path>/jais-2.1R2.0-signed.tgz`**.

The AI-Scripts install package is installed on the device.



NOTE: When you install AI-Scripts in the Juniper Networks QFX3000 device, ensure that you install the events scripts only on the controller. The controller installs AI-Scripts on the node devices and enables all the events.

- Related Documentation**
- [Installing an Event Profile on Devices Using Service Now on page 59](#)
 - [Adding a Script Bundle to Service Now on page 87](#)

Uninstalling Event Profiles from Devices

You can use Service Now to remove event profiles from devices. You cannot remove event profiles from devices that do not have proper login credentials. Service Now uses Device Management Interface (DMI) to install and remove event profiles on devices. DMI is an extension to the NETCONF network management protocol.



NOTE: While operating in partner-proxy mode, you cannot remove event profiles from a connected member's device.

To remove event profiles from devices:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

2. Select the devices from which you want to remove event profiles, and select **Uninstall Event Profile** from either the **Actions** drawer or the right-click menu.

A message box appears asking you to confirm the deletion.

3. Click **Submit**.

This event profiles are removed from the selected devices.

To view the status of this task, click the job ID link. The Manage Jobs page displays the status of the job. Double-click the job to view information about each step of the removal.

Related Documentation

- [AI-Scripts Overview on page 85](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)

Exporting Device Data in CSV and Excel Format

You can export Service Now device data in CSV and Excel file formats. A CSV file is a plaintext file that stores each data record separated by a comma. The XML file contains the hardware components installed in the selected device.

To export the device data in CSV and Excel format:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

2. Select the device whose data you want to export, and select **Export Devices** from either the **Actions** drawer or the right-click menu.

The **Export Devices** dialog box displays the links to the CSV and Excel files.

3. Select the links to save the files in CSV and Excel file formats.

Related Documentation

- [Service Now Devices Overview on page 55](#)
- [Deleting a Device on page 67](#)
- [Adding Devices to Auto Submit Policies on page 69](#)

Exporting Inventory Information in CSV Format

You can export Service Now end-customer device inventory information in CSV and Excel file formats. A CSV file is a plain text file that stores each data record separated by a comma.

To export the inventory information:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.
The Service Now Devices page appears.
2. Select the device whose data you want to export.
3. The **Export Inventory** dialog box appears you to select
The **Export Inventory Job Status** dialog box appears and shows the job status.
4. After the job is complete, click **Download** to open the files in CSV and Excel file formats.
The information appears according to device, item, model number, part number, serial number, service SKU, contract end, EOL status, EOL replacement part, EOL date, and description.



NOTE: The device inventory of end-customer devices takes one day to be reflected in the mode.

Related Documentation

- [Service Now Devices Overview on page 55](#)
- [Deleting a Device on page 67](#)
- [Adding Devices to Auto Submit Policies on page 69](#)
- [Viewing Exposure on page 64](#)

Viewing Exposure

The Service Now Devices page displays a bang (!) icon next to the organization associated with devices that are exposed to known issues.

Using Service Now, you can view details of these exposed devices. The details include the device name, Junos OS version, script bundle, and associated information messages as well as a link to the problem report (PR) and a description of the problem.



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

To view device exposures to known issues:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

2. Select the device that is exposed and click **View Exposure** from either the **Actions** drawer or the right-click menu.

The View Exposure page appears and displays information according to device name, product, version, PR, and PR synopsis.

3. Click **Return to Device View** to go back to the Service Now Devices page.

Related Documentation

- [Service Now Devices Overview on page 55](#)
- [Adding Devices from the Platform on page 58](#)
- [Deleting a Device on page 67](#)
- [Adding Devices to Auto Submit Policies on page 69](#)

Generating On-Demand Incidents

Using Service Now, you can create Juniper Message Bundles (JMBs) for specific devices without having to wait for an event to trigger an incident. These JMBs are called on-demand incidents. When you submit an on-demand incident, Service Now calls an on-demand incident profile, which triggers an event and generates the incident. These profiles are predefined by Juniper Networks and contain information such as type of incident and the remote procedure calls (RPCs) used to trigger the incident.



NOTE: To create an on-demand incident, you must first install AI-Scripts Releases 3.2 R1 and later on the device.

You cannot create on-demand incidents for Juniper Networks QFX3000 devices.

To generate incidents on demand:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

2. Select the device for which you want to generate the incident, and click **Create On-Demand Incident** from either the **Actions** drawer or the right-click menu.

You can create on-demand incidents for 1 to 5 devices simultaneously

The On-demand Incident dialog box appears.

Figure 11: On-demand Incident Dialog Box



The dialog box is titled "On-demand Incident" and contains the following elements:

- Add CC to Case:** A section with an "Add Email" button, a "Delete" button, and a list box labeled "Email List". Below the list box is a checkbox labeled "Enter Email Id".
- Follow Up Method:** A dropdown menu currently showing "Please select ...".
- Priority:** A dropdown menu currently showing "Low".
- Add Comments to Synopsis:** A large text input field.
- Add Comments to Description:** A large text input field.
- Schedule at a later time:** A checkbox with a calendar icon.
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

- Click the **Enter Email Id** field to enter an e-mail ID, and enter the e-mail ID in the format user@example.com.
To add multiple e-mail IDs, or delete them, use the **Add Email** and **Delete** buttons, respectively.
- Select how you can receive updates about the case from the **Follow Up Method** list. The available options are **Email Full Text Update**, **Email Secure Web Link**, and **Phone Call**.
- Select the priority of the case from the **Priority** list. The available options are **Critical**, **High**, **Medium**, and **Low**. The default priority is **Medium**.
- Enter your comments about the problem synopsis and a description of the case in the **Add Comments to Synopsis** and **Add Comments to Description** fields, respectively. Ensure that your comments are less than 1,028 characters.



NOTE: The values for the fields listed in steps 3 through 5 are already defined based on the incident that is generated by the selected profile. You can modify these values if needed.

- Click **Submit**. A **Job Information** dialog box appears and displays the job ID.

You can click the job ID to go to **Create On-demand Incident** job on the Manage Jobs page. Double-click the job to open the **Create On-demand Incident Status** dialog box (Figure 12 on page 67), which displays information about the job such as profile used in the incident, hostname, job status, and reason for the incident.

Figure 12: Create On-demand Incident Status Dialog Box

Create On-demand Incident Status			
Profile Name	Host Name	Status	Reason
General	EX4200.24T.180	Failed	OP Script execution failed on device 229656. Src File: on-Demand.slax Please verify that the AI Script with version 3.1R2 or higher is installed on device. Message from device : Details: Operational RPC Command Results operationalCmd Failed . error invalid script name: on-demand.slax invalid script name: on-demand.slax
General	SRX210H-SN	Failed	OP Script execution failed on device 229660. Src File: on-Demand.slax Please verify that the AI Script with version 3.1R2 or higher is installed on device. Message from device : Details: Operational RPC Command Results operationalCmd Failed . error no op scripts configured no op scripts configured
General	srx3600_50_75	Success	On-demand JMB was generated for device and is available in the Incidents table under Service Central.
General	srx3600_50_76	Success	On-demand JMB was generated for device and is available in the Incidents table under Service Central.

Related Documentation

- [Service Now Devices Overview on page 55](#)
- [Adding Devices from the Platform on page 58](#)
- [Deleting a Device on page 67](#)
- [Adding Devices to Auto Submit Policies on page 69](#)
- [Viewing Exposure on page 64](#)

Deleting a Device

When you delete a device, the device is deleted from Service Now, but it is not deleted from the Junos Space Platform. The incidents and JMBs related to the device are also deleted.

To delete a device from Service Now:

- From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page lists the Service Now devices.

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

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

3. Click **Delete**.

The selected device is deleted from the Service Now database and is no longer displayed on the Service Now Devices page.

**Related
Documentation**

- [Service Now Devices Overview on page 55](#)
- [Adding Devices from the Platform on page 58](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)
- [Modifying Device Groups on page 52](#)

Associating Devices with a Device Group

Using Service Now you can associate devices with device groups which are directly associated with Service Now organizations. Associating devices with device groups helps you group devices under different site IDs.

If Service Now is configured as a partner proxy, you can combine devices that are directly connected to Service Now and devices from a connected member in a single Service Now device group. Alternately, you can create a device group for each connected member and associate them to Service Now organizations dedicated to each connected member. This kind of grouping enables you track and organize technical support cases for a single end-customer using different organizations (site IDs).

To associate devices with device group:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page lists the Service Now devices.

2. Select the device that you want to associate with a device group and select **Associate Device Groups** from either the **Actions** drawer or the right-click menu.

The **Associate Device Groups** dialog box appears.

3. From the **Device Group** list, select the device group that you want to associate with the selected device.

4. Click **Submit**.

The device is associated with the selected device group. You can verify the changes on the Service Now Devices page, in the **Device Group** column.

**Related
Documentation**

- [Service Now Devices Overview on page 55](#)
- [Adding Devices from the Platform on page 58](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)

- [Modifying Device Groups on page 52](#)
- [Adding Devices to Auto Submit Policies on page 69](#)

Adding Devices to Auto Submit Policies

You can associate devices with auto submit policies to enable automatic submission of incidents that occur on the devices to JSS. To associate devices with an auto submit policies, you must first create an auto submit policy (see [“Creating an Auto Submit Policy” on page 100](#)).

To add devices to an auto submit policy:

1. From the Service Now taskbar, select **Administration > Service Now Devices**.

The Service Now Devices page appears.

2. Select the devices that you want to include in auto submit policies, and select **Add to Auto Submit Policy** from either the **Actions** drawer or the right-click menu.

The **Add to Auto Submit Policy** dialog box displays all auto submit policies and selected devices.

Figure 13: Add to Auto Submit Policy Page

Create Auto Submit Policy

Policy Name: !

Show: **By Organization**

Organization: Gooma Alcatel [Show Selected Devices](#)

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle
Gooma	DeviceGroup	Elmo	J1213	M7I	11.2B3	11.2R1.1
Gooma	DG	SRX-5600	JN11198B8AGB	SRX5600	11.1B1	Unavailable
Gooma	DG	nms3-f	A2831	M10I	10.2R1	Unavailable
Alcatel	AlcatelDG	ex-4200-50-182	BM0210435487	EX4200-24T	11.2B3	11.2R1.1
Alcatel	AlcatelDG	mx480-2-re0	JN11AFF42AFB	MX480	11.2B3	11.2R1.1
Gooma	DG	Device1111	F00000010011	MX960	9.5R2	
Gooma	DG	Device1117	F00000010017	MX960	9.5R2	
Gooma	DG	Device1115	F00000010015	MX960	9.5R2	
Gooma	DG	Device1120	F00000010020	MX960	9.5R2	

Page 1 of 5 | [Next](#) [Cancel](#) | Displaying 1 - 25 of 105

3. Select the auto submit policies with which you want to associate the selected devices.
4. To associate the devices with the selected auto submit policies, click **Add**.

To dissociate the devices with the selected auto submit policies, click **Remove**.

The Service Now Devices page appears.

5. (Optional) To verify your changes, navigate to the View Auto Submit Policy page and view the list of devices with which the selected auto submit policies were associated.

Related Documentation

- [Auto Submit Policy Overview on page 99](#)
- [Adding Devices from the Platform on page 58](#)

- [Service Now Devices Overview on page 55](#)

CHAPTER 13

Event Profiles and AI-Scripts

- [Event Profiles Overview on page 71](#)
- [Adding an Event Profile on page 73](#)
- [Cloning an Event Profile on page 78](#)
- [Deleting Event Profiles on page 79](#)
- [Viewing an Event Profile on page 80](#)
- [Pushing an Event Profile to Devices on page 80](#)
- [Displaying Devices Associated with an Event Profile on page 83](#)
- [Setting an Event Profile as Default on page 83](#)
- [Exporting Events Data in Excel Format on page 84](#)
- [AI-Scripts Overview on page 85](#)
- [Adding a Script Bundle to Service Now on page 87](#)
- [Setting a Script Bundle as Default on page 88](#)
- [Deleting a Script Bundle from Service Now on page 88](#)

Event Profiles Overview

An event profile is a set of event scripts selected from an AI-Scripts bundle. Using event profiles, you can specify the event scripts that you want to install on Service Now devices.

To create an event profile, you need an AI-Scripts bundle from which you can select the event scripts that you want to associate with the event profile. The set of event scripts can be updated using the latest AI-Scripts bundles.

When you install Service Now, the latest AI-Scripts bundle is preloaded and displayed on the Manage Script Bundles page. You can also download other AI-Scripts bundles from the Juniper Networks software download site and upload them to Service Now (see [“Adding a Script Bundle to Service Now” on page 87](#)).

In Service Now, there is always an event profile and an AI-Scripts bundle that is set as the default. The default event profile is always associated with an AI-Scripts bundle. For new Service Now installs or upgrades, the default event profile is associated with the preloaded AI-Scripts bundle.

After installing or upgrading Service Now, you can add additional AI-Scripts bundles and set any AI-Scripts bundle and event profile as the default. The default script bundle is automatically selected while creating a new event profile and the default event profile is automatically selected while installing an event profile on devices.

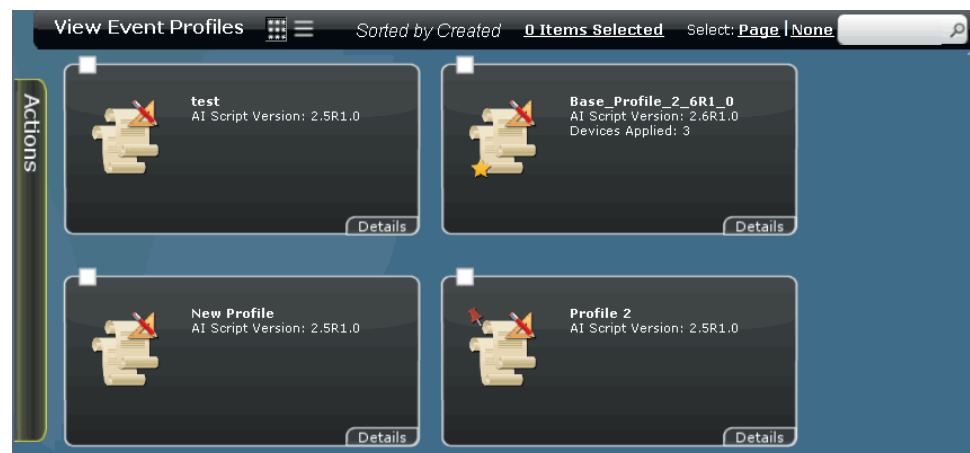


NOTE: Read the KB article, <http://kb.juniper.net/KB19155>, before installing AI-Scripts on devices.

Service Now allows you to clone an existing event profile by modifying its name, description, script bundle, set of included event scripts, and event script priorities. Cloning an event profile allows you to make changes without losing the original event profile. After you make your modifications, you can save the cloned event profile and apply it over the original event profile for devices where the original event profile was installed. You can also install the new event profile on any other devices. The priority values of event scripts determine the priority shown in the JMBs generated for a Service Now event. After you install event profiles on devices, you can filter and display only the devices that are associated with a specific event profile. Service Now also enables you to export events data that is specific to an event profile in Excel format and delete event profiles that are not associated with devices.

In Service Now, event profiles are displayed on the View Event Profiles page ([Figure 14 on page 72](#)). The tabular view of the View Event Profiles page displays information about the event profile including the total number of incidents generated per event in the event profile, the total number of active events, the total number of inactive events, the number of devices on which the event profile is installed, most active events, least active events, and inactive events. The default event profile and the event profiles that are installed on the devices are represented by two unique icons. For example, as shown in [Figure 14 on page 72](#), Profile 2 is the default event profile, and Base_Profile_2.6R1_0 is an event profile that is installed on the devices.

Figure 14: View Event Profiles Page



Using the **Event Profiles** workspace, you can perform the following tasks:

- Add an event profile
- Push an event profile to devices
- Display devices associated with an event profile
- Set an event profile as default
- Export events data in Excel format
- View an event profile
- Clone an event profile
- Delete event profiles

Related Documentation

- [Installing an Event Profile on Devices Using Service Now on page 59](#)
- [Adding an Event Profile on page 73](#)
- [Pushing an Event Profile to Devices on page 80](#)
- [Displaying Devices Associated with an Event Profile on page 83](#)
- [Setting an Event Profile as Default on page 83](#)
- [Exporting Events Data in Excel Format on page 84](#)
- [Viewing an Event Profile on page 80](#)
- [Cloning an Event Profile on page 78](#)
- [Deleting Event Profiles on page 79](#)

Adding an Event Profile

An event profile is a set of scripts that are selected from an AI-Scripts bundle. Using event profiles, you can specify the event scripts you want to install on the devices. To add an event profile, you can use the default AI-Scripts bundle that is available when you install Service Now, or upload a new AI-Scripts bundle (see [“Adding a Script Bundle to Service Now” on page 87](#)).

After you add a script bundle to Service Now, to be able to install the script bundle on the devices, you must create an event profile using this script bundle.

To add an event profile:

1. From the Service Now taskbar, select **Administration > Event Profiles > Add Event Profile**.

The Add Event Profile page appears.

Figure 15: Add Event Profile Page

For a description for the fields displayed on this page, see [Table 9 on page 75](#).

Table 9: Add Event Profile Page Field Descriptions

Field	Description
Profile Name	Name of the event profile that you specify.
Description	Explanation that you specify about the event profile.
Script Bundle	List of AI-Scripts bundles that are available in Service Now. This consists of the default AI-Scripts bundle that is available with Service Now and the ones that you upload.
Find Events	Filters the displayed list of events according to the value you select from the list.
Show Selected Events	Shows all the events that you have selected.
Description of the columns in the Add Event Profiles page	
Event Synopsis	Name used to identify the event script.
Type	Type of event that triggers the event script: <ul style="list-style-type: none"> • Hardware failure • Software failure • Resource Exhaustion
Sub Type	Detailed description for the type of event that triggers the event script. For example, file system error, communication error, socket failure, excessive memory utilization, database failure, session error, memory allocation error, initialization error, process error, and so on.

Table 9: Add Event Profile Page Field Descriptions (*continued*)

Field	Description
Priority	Priority level of the event script. The values are: 1. Low 2. Medium 3. High 4. Critical
Category	Type of event script.

2. Enter an event profile name.

3. (Optional) Enter a description for the event profile.

4. Select a script bundle from the **Script Bundle** list.

By default, the script bundle that is set as the default is automatically selected and you can modify this selection if required.

5. (Optional) To add a new script bundle, click **Add Script Bundle** (see [“Adding a Script Bundle to Service Now” on page 87](#)).

6. (Optional) To look for specific events, use the **Find Events** field.

7. Click **Submit**.

An event profile is created with your specifications. To verify, you can view the details of the event profile displayed on the Manage Event Profiles page.

The **Save Event Profile** dialog box appears.

8. Click one of the following links based on the required results.

Link	Result
Apply this profile to original set of devices	The Potential Exposure to Known Issues page appears and displays information about the selected set of devices. A bang (!) icon is placed next to devices that risk the chance of exposure.

Figure 16: Potential Exposure to Known Issues Page



1. (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.
2. (Optional) To view a device's exposure to known issues, click the respective link displayed in the **Exposure** column. The View Exposure page appears and displays the known issues associated with the respective device. Click **Return to Potential Exposure** to continue.
3. Click **Continue**.
A confirmation pop-up box lists the final list of devices on which the selected event profile must be installed.
You can remove devices from the list by clearing the check boxes of the devices you want to delete.
4. Click **Install**.
The selected event profile is installed on the devices with which it is associated, and the Service Now Devices page appears.

Apply this profile to devices manually	<p>The Push to Devices page appears. Here you can select Service Now devices on which you want to install the event profile.</p> <p>For more information, see "Pushing an Event Profile to Devices" on page 80.</p>
Return to the Profiles Page	The event profile installation task is canceled, and the Manage Event Profiles page appears.

Related Documentation

- [Pushing an Event Profile to Devices on page 80](#)
- [Displaying Devices Associated with an Event Profile on page 83](#)
- [Event Profiles Overview on page 71](#)

Cloning an Event Profile

Service Now enables you to clone an existing event profile and modify its priority to create another event profile. After you clone an event profile, you can redeploy the event profile, or deploy the event profile on new devices. When you create a clone of an event profile, the event profile name is appended with **Copy of**.

To clone an event profile:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Manage Event Profiles page appears.
2. Select the event profile that you want to clone, and select **Clone** from either the **Actions** drawer or the right-click menu.

The **Clone Event Profile** dialog box displays the attributes of the event profile that you selected.
3. Select the events that you want to include as part of the event profile.
4. (Optional) To lsearch for specific events, enter the name of the event in the **Find Events** field.
5. Make your modifications to the priority of the event profile. The values are:
 1. Low
 2. Medium
 3. High
 4. Critical

6. Click **Submit**. The event profile is created and the **Save Event Profile** dialog box appears.
7. Click one of the following links based on the required results.

Link	Result
Apply this profile to original set of devices	<p>The Potential Exposure to Known Issues page displays information about the selected set of devices. A bang (!) icon is placed next to devices, associated with the event profile, that risk the chance of exposure.</p> <ol style="list-style-type: none"> 1. (Optional) To export device data in an Excel format, click Export Devices with Exposure to Excel. 2. (Optional) To view a device's exposure to known issues, click the respective link displayed in the Exposure column. The View Exposure page appears and displays the known issues associated with the respective device. Click Return to Potential Exposure to continue. 3. Click Continue. A confirmation pop-up box lists the final list of devices on which the selected event profile must be installed. You can remove devices from the list by clearing the check boxes of the devices you want to delete. 4. Click Install. The selected event profile is installed on the devices with which it is associated, and the Service Now Devices page appears.
Apply this profile to devices manually	<p>The Push to Devices page appears. Here you can select Service Now devices on which you want to install the event profile.</p> <p>For more information, see "Pushing an Event Profile to Devices" on page 80.</p>
Return to the Profiles Page	The event profile installation task is canceled, and the Manage Event Profiles page appears.

- Related Documentation**
- [Pushing an Event Profile to Devices on page 80](#)
 - [Event Profiles Overview on page 71](#)

Deleting Event Profiles

Using Service Now, you can delete multiple event profiles. You can delete an event profile only if it is not associated with a device.



NOTE: When you delete the default event profile, the latest created profile is automatically set as the default.

To delete event profiles:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Manage Event Profiles page appears.

2. Select the event profiles that you want to delete, and select **Delete** from either the **Actions** drawer or the right-click menu.

The **Delete Event Profiles** dialog box displays the list of event profiles that you selected.

3. Click **Delete** to confirm.
The selected event profiles are deleted. To verify, you can check the list of event profiles displayed on the Manage Event Profiles page.

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 83](#)
- [Cloning an Event Profile on page 78](#)
- [Pushing an Event Profile to Devices on page 80](#)

Viewing an Event Profile

Using Service Now, you can view an event profile's name, its description, and the scripts that are associated with it.

To view the event scripts that are part of an event profile:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Manage Event Profiles page appears.
2. Select the event profile whose details you want to view, and select **View Events** from either the **Actions** drawer or the right-click menu.

The Event Profiles page displays the event profile's name, its description, and the scripts that are associated with it. The event script details includes the event script names, types, sub types, descriptions, priorities, occurrences in the last 90 days, the total number of occurrences, the number of unique devices, and the number of top devices.

3. Click **OK** to return to the Manage Events page.

Related Documentation

- [Exporting Events Data in Excel Format on page 84](#)
- [Cloning an Event Profile on page 78](#)
- [Pushing an Event Profile to Devices on page 80](#)

Pushing an Event Profile to Devices

An event profile is a set of event scripts that are selected from a script bundle. When you push an event profile onto Juniper Networks devices, these event scripts are installed on the devices. The event scripts provide the information needed to automatically detect and report problem (incident) and information events. Service Now uses Device Management Interface (DMI) to install and remove event profiles on devices. DMI is an extension to the NETCONF network management protocol.

When you install event profiles on individual systems (chassis) with dual Routing Engines, Service Now installs the event profiles on both the primary and backup Routing Engines.



NOTE: While operating in partner-proxy mode, you cannot push event profiles to a connected member's device.

To push an event profile to devices:

1. From the Service Now taskbar, select **Administration > Event Profiles**.

The View Event Profiles page appears.

2. Select the event profile that you want to push to devices, and select **Push to devices** from either the **Actions** drawer or the right-click menu.

The **Push to Devices** dialog box appears (see [Figure 17 on page 81](#)).

Figure 17: Push to Devices Dialog Box

Organization	Device Group	Hostname	Serial Number	Product	Version	Script bundle	Event Profile
JSpace_Partner	DevGroup	nms3-f	A2831	M101	10.4R7.5		
JSpace_Partner	DevGroup	snk3600_50_75	AB3510AA0022	SRX3600	11.2R3.2	3.1R1.1	Base_Profile_3_1R...
JSpace_Partner	DevGroup	elmo	71213	M71	11.1R2.3	3.0R1.0	Prof_30R1
JSpace_Partner	DevGroup	ex-4200-50-182	BM0210435487	EX4200-24T	11.3R1.5	3.1R1.1	Base_Profile_3_1R...
JSpace_Partner	DevGroup	mx960-77-48	JN10EAD81AFA	MX960	10.4R5.5	3.1R1.1	Base_Profile_3_1R...
JSpace_Partner	DevGroup	snk650_191	A34410AA0031	SRX 650	11.1R5.4		
JSpace_Partner	DevGroup	SS0550	0158102005000115	SS0550			

☐ Never store Script Bundle files on device (if selected roll-back option will not be available)
☐ Remove Script Bundle files after successful install
☐ Schedule at a later time

Submit Cancel



NOTE: You can install event profiles only on devices for which you can specify correct login credentials and that belong to a device group.

3. Select the devices on which you want to install the event profile.
4. (Optional) If you do not want to save a copy of the event profile after it is installed on the device, select the **Never store Script Bundle files on device (if selected roll-back option will not be available)** check box.
5. (Optional) If you want to remove the script bundle from the device, after it is installed, select the **Remove Script Bundle files after successful install** check box.
6. (Optional) If you want to schedule a time for installation, select the **Schedule at a later time** check box, and specify the **Date and time** for the installation. The installation process begins automatically at the time you specify.
7. Click **Submit**.

The Potential Exposure to Known Issues page appears and displays information about the selected set of devices. A bang (!) icon is placed next to devices associated with the event profile that risk the chance of exposure.

Figure 18: Potential Exposure to Known Issues Page

Device Name	Serial Number	Product	Version	Exposure
nm33-f	A2831	M101	11.2R3.3	None
sr3600_50_75	A63510AA0022	SRx3600	11.2R3.2	Click
elmo	31213	M71	11.1R2.3	Click
ex-4200-50-182	8M0210435487	EX4200-24T	11.3R1.5	None
mx960-77-48	JN10EAD81AFA	MX960	10.4R5.5	None
sr650_191	A34410AA0031	SRx 650	11.1R5.4	None
S50550	0158102005000115	S50550	6.3.0R5.0	None

8. (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.
9. (Optional) To view device's exposure to known issues, click the respective link displayed in the **Exposure** column. The View Exposure page appears and displays the known issues associated for the respective device.

Click **Return to Potential Exposure** to continue.

10. Click **Continue**.

A confirmation pop up box lists the final list of devices on which the selected event profile must be installed.

You can remove devices from the list by clearing the check boxes of the devices you want to delete.

11. Click **Install**.

The event profile installation task is performed when scheduled and the **Job Information** dialog box displays the job ID.

To view the status of this task, click the job ID link. The Manage Jobs page displays the status of the job. The **Device Details** dialog box also displays the status of script installation for the selected devices.

If you have installed the event profile on a dual Routing Engine, the results (displayed on the Manage Jobs page) shows the status for both the primary Routing Engine and the backup Routing Engine. The status of the job says **Failed** if the installation fails on either of the Routing Engines.

12. Click **OK**.

The View Event Profiles page appears.

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 83](#)

- [Event Profiles Overview on page 71](#)
- [Adding an Event Profile on page 73](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)
- [Cloning an Event Profile on page 78](#)
- [Viewing Exposure on page 64](#)

Displaying Devices Associated with an Event Profile

Using Service Now, you can view only those devices that are associated to a specific event profile. This task is disabled when you select an event profile that is not associated to any device.

To display devices associated to an event profile:

1. From the Service Now taskbar, select **Administration > Event Profiles**.

The View Event Profiles page appears.

2. Select the event profile to view the devices associated with it, and select **Show Associated Devices** from either the **Actions** drawer or the right-click menu.

The Manage Service Now Devices page displays only the devices that are associated with the event profile that you selected.

Related Documentation

- [Viewing an Event Profile on page 80](#)
- [Installing an Event Profile on Devices Using Service Now on page 59](#)
- [Adding an Event Profile on page 73](#)
- [Pushing an Event Profile to Devices on page 80](#)

Setting an Event Profile as Default

Service Now allows you to set an event profile as the default. When you select devices on which you want to install an event profile, the default event profile is automatically selected as the event profile that must be installed. The default event profile is represented by a unique icon on the View Event Profiles page. If you delete the default event profile, the latest event profile is automatically set as the default.

To set an event profile as the default:

1. From the Service Now taskbar, select **Administration > Event Profiles**.
The Manage Event Profiles page appears.
2. Select the event profile that you want to set as the default, and select **Set as Default** from either the **Actions** drawer or the right-click menu.

The **Set As Default Profile** dialog box prompts you for a confirmation

3. Click **Confirm**.

The selected event profile is set as the default and is automatically selected as the event profile that must be installed when you select devices (Manage Service Now Devices page) on which you want to install an event profile. The default event profile (for example, Profile 2 in [Figure 19 on page 84](#)) is represented by a unique icon on the View Event Profiles page.

Figure 19: View Event Profiles Page

	Name	Description	AI Script Version	Created By	Created	Events Included	Events Excluded	Devices
	test		2.5R1.0	super	Jan 26, 2011 7:05:48 PM IST	383	0	0
	Base_Profile	Base Profile for Bundle Version: 2.6R1.0	2.6R1.0	Service Now	Jan 24, 2011 6:22:33 PM IST	376	0	2
	New Profile	New Profile description	2.5R1.0	super		383	0	0
	Profile 2	Profile 2 description	2.5R1.0	super		20	363	1

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 83](#)
- [Cloning an Event Profile on page 78](#)
- [Pushing an Event Profile to Devices on page 80](#)

Exporting Events Data in Excel Format

Service Now enables you to export events data into Excel file format, and save it on your local file system.

To export events data into Excel file format:

1. From the Service Now taskbar, select **Administration > Event Profiles**. The Manage Event Profiles page appears.
2. Double-click the event profile whose event activity you want to export into the Excel file format.
The **Event Profile Detail** dialog box displays details about the event activity that are associated to the event profile that you selected.
3. Click the **Export events to Excel** link.
The **Opening ProfileEvents.xls** dialog box allows you to open or save the Excel file.
4. To open the Excel file, select **Open with**.
To save the Excel file on your local file system, select **Save File** and navigate to the folder where you want to save the Excel file.
5. Click **OK**.
The information that appears in five separate tabs in the **Event Profile Detail** dialog box, appears in five separate worksheets in the Excel file.

Related Documentation

- [Displaying Devices Associated with an Event Profile on page 83](#)
- [Cloning an Event Profile on page 78](#)

- [Pushing an Event Profile to Devices on page 80](#)

AI-Scripts Overview

Advanced Insight Scripts (AI-Scripts) provide the intelligence that devices need to automatically detect and report incident and intelligence events to ensure maximum network uptime.

When AI-Scripts are installed on a device, the device is said to be AIS-enabled. It can then automatically detect and report incidents and informational JMBs. This helps to ensure maximum network uptime.

This section contains the following topics:

- [What AI-Scripts Do on page 85](#)
- [Events Detected by AI-Scripts on page 86](#)
- [JMB Contents on page 87](#)

What AI-Scripts Do

AI-Scripts perform the following functions:

- React to specific incident events that occur on devices and provide relevant information about the problems for analysis.
- Periodically collect data on events that can be used to predict and prevent risks in the future.
- Package all incident and intelligence event data into a structured format called a Juniper Message Bundle (JMB) and place it in the predefined location on the device memory so that it can be collected and displayed by the second component in the Service Automation solution, Junos Space Service Now. Service Now can be configured to send event data to Juniper Support Systems (JSS), the third component in the Service Automation solution. JSS collects incident and intelligence information from Service Now and sends intelligence information back to Service Now specifically for your network.



NOTE: Service Now uses the loopback interface on the device to collect JMBs whenever an event occurs. A device running Junos OS may have trouble sending JMBs to Service Now if the device does not allow traffic to the local host address (127.0.0.1).

You (the administrator) can fix this by adding the following firewall rule to the device:

```
set firewall family inet filter scp-block term ais-scp from
source-address 127.0.0.1/32
set firewall family inet filter scp-block term ais-scp from
destination-address 127.0.0.1/32
set firewall family inet filter scp-block term ais-scp from protocol
tcp
set firewall family inet filter scp-block term ais-scp from port 22
set firewall family inet filter scp-block term ais-scp then accept
```

```
Router001# show firewall family inet filter scp-block term ais-scp
from {
source-address {
127.0.0.1/32;
}
destination-address {
127.0.0.1/32;
}
protocol tcp;
port 22;
}
then accept;
```

If you do not want to use the loopback address, you can modify the configuration to use the device management IP address instead of the loopback address to collect JMBs.

AI-Scripts operate in a reactive (incident-driven) mode. When a trigger event occurs and is detected on a device, an AI-Script is executed. The AI-Script builds a JMB with event and router data, and sends it to Service Now. Each AI-Script corresponds to a specific device event. The list of device events that can be detected and reported evolves over time.

You can also create JMBs for specific devices without having to wait for an event to trigger an incident. These JMBs are called on-demand incidents. When you submit an on-demand incident, Service Now calls a predefined on-demand incident profile, which triggers an event and generates the incident.

Events Detected by AI-Scripts

AI-Scripts detect the following types of events:

- Common software events, including daemon and Packet Forwarding Engine crashes
- Common hardware events, such as PIC alarms
- Hardware platform-specific events, such as ASIC issues

JMB Contents

The JMB for incidents and informational JMBs contains the following:

- Manifest—basic router and event data
- Trend data (only for informational JMBs)—device counters, statistics, and settings
- Attachments—show command output for the incident event.

Related Documentation

- [Adding a Script Bundle to Service Now on page 87](#)
- [Deleting a Script Bundle from Service Now on page 88](#)

Adding a Script Bundle to Service Now

The Manage Script Bundles page provides a central point for managing script bundles (also known as AI-Scripts install packages) that have been downloaded from the Juniper Networks software download site. The script bundles must be located locally to the system running the Service Now application. You need Service Now Admin privileges to add a script bundle.

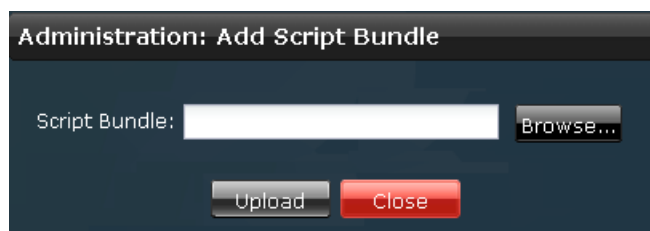
After you add a script bundle to Service Now, to be able to install the script bundle on devices you must first create an event profile using this script bundle. See [“Adding an Event Profile” on page 73](#).

To add a script bundle:

1. From the Service Now taskbar, select **Administration > Script Bundles > Add Script Bundle**.

The Add Script Bundle page appears as shown in [Figure 20 on page 87](#).

Figure 20: Add Script Bundle Dialog Box



2. Click **Browse**.

The File Upload window appears.

3. Locate the script bundle and click **Upload**.

The selected script bundle is uploaded into Service Now and appears on the Manage Script Bundles page.

Related Documentation

- [AI-Scripts Overview on page 85](#)

- [Deleting a Script Bundle from Service Now on page 88](#)

Setting a Script Bundle as Default

Service Now allows you to set a script bundle as the default. When you create an event profile, the default script bundle is automatically selected as the script bundle from which you select event scripts to associate with the event profile. The default script bundle is represented by a unique icon on the Manage Script Bundles page. If you delete the default script bundle, the latest script bundle to be uploaded is automatically set as the default.

To set a script bundle as the default:

1. From the Service Now taskbar, select **Administration > Script Bundles**.
The Manage Script Bundles page lists the available script bundles.
2. Select the script bundle that you want to set as the default, and select **Set as Default Bundle** from either the **Actions** drawer or the right-click menu.
The **Set as Default Bundle** dialog box prompts you to confirm.
3. Click **Confirm**.
The selected script bundle is set as the default and is represented by a unique icon on the Manage Script Bundles page.

Related Documentation

- [Manually Installing AI-Scripts on Devices on page 62](#)
- [Adding a Script Bundle to Service Now on page 87](#)
- [Deleting a Script Bundle from Service Now on page 88](#)

Deleting a Script Bundle from Service Now

With Service Now Admin privileges, you can delete script bundles.



NOTE: You cannot delete the preloaded script bundle that is available with Service Now.

To delete a script bundle:

1. From the Service Now taskbar, select **Administration > Script Bundles**.
The Manage Script Bundles page lists the available script bundles.
2. Select the script bundle that you want to delete, and select **Delete Script Bundles** from either the **Actions** drawer or the right-click menu.
The **Delete AI-Scripts** dialog box prompts you to confirm the deletion.
3. Click **Delete**.

Service Now deletes the script bundle from the database and returns to the Manage Script Bundles page.

- Related Documentation**
- [AI-Scripts Overview on page 85](#)
 - [Adding a Script Bundle to Service Now on page 87](#)

CHAPTER 14

Global Settings

- [Configuring Global Settings on page 91](#)
- [Adding an SNMP Server on page 94](#)
- [Editing and Deleting an SNMP Server on page 96](#)
- [Configuring Proxy Server Settings on page 96](#)

Configuring Global Settings

You can use the Service Now global settings to perform the following tasks:

- Verify the connection status of Service Now to Juniper Support Systems (JSS) or Service Now to (from end-customer mode).
- (For end-customers) Connect to Service Now.

Using the Service Now Global Settings page, a Service Now end-customer can connect to a partner's Service Now application. When the Service Now application of an end-customer connects to that of a partner, Junos Space uses a self-signed security certificate. Although Junos Space does not trust this method of identification, it automatically accepts the certificate to ensure that the communication between the partner and the end-customer is encrypted. Once you connect to the partner's Service Now application, you enter end-customer mode. After Service Now begins to operate in the end-customer mode, you cannot revert to standard or modes. After you connect to the Service Now application, you can add an organization using the credentials provided by the partner. See [“Adding an Organization” on page 43](#). After the connection of the organization is validated, you can submit incidents and iJMBs to, and open cases with, the Service Now partner.

For more information about standard, partner, and end-customer modes, see [“Service Now Modes” on page 19](#).

To configure Service Now global settings:

1. From the Service Now taskbar, select **Administration > Global Settings**.

The Global Settings page appears.

Figure 21: Global Settings Page

2. Enter the global settings as described in [Table 10 on page 93](#).

3. Select one of the following options:

- **Online Mode**—Click to use Service Now in the online mode.
- **End-Customer**—Enter the IP address or hostname of the Service Now partner-proxy that can be used to send information to and receive information from the partner-proxy.
- **Offline Mode**—Click **Browse** to open the File Upload window. Select the license file and click **Upload**. After you upload the license file and submit the general settings, message **Service Now offline mode is enabled** appears.



NOTE: Service Insight is disabled when Service Now is in the offline mode.



NOTE: You can move from offline to online mode by selecting the Online option in the Global Settings page after you first create or modify the organization using partner credentials.

4. Click **Submit** to save the global settings and update Service Now.



NOTE: Use the Manage SMTP Servers task to specify your SMTP settings. You can navigate to the task by selecting **Network Application Platform** from the Application Chooser and then selecting **Administration > Manager SMTP Server** from the Platform taskbar.

Table 10 on page 93 describes the fields displayed in the tabular view of the Global Settings page.

Table 10: Global Settings Parameters

Name	Description	Privileges	Range/Length	Default
Outbound e-mail address	E-mail address that the recipients see (for example, <code>exampleservicenow@juniper.net</code>)			
Device Snapshot Purge Time (in days)	Number of days the device snapshots are stored in the Service Now database before they are deleted.	Service Now administrator privileges	—	90 to 365 days
Incident Purge Time (in days)	Number of days the incidents are stored in the Service Now database before they are deleted.	Service Now administrator privileges	—	90 to 365 days
Event Profile Jobs Purge Time (in days):	Number of days the event profile jobs are stored in the Service Now database before they are deleted.	Service Now administrator privileges	—	90 to 365 days
Connection Status	<p>Status of connection from Service Now to JSS.</p> <p>If Service Now is operating in end-customer mode, the connection status between Service Now and the partner-proxy appears</p>	Service Now Partner	<ul style="list-style-type: none"> • Success — URL is responsive • No route to host • Connection refused • The Home Base server is temporarily unable to service your request 	Blank

Table 11 on page 93 describes the command buttons on the Global Settings page.

Table 11: Global Settings Command Buttons

Button Name	Description	Privileges	Enabled/Disabled	Results
Submit	Saves any modified Service Now global settings and updates the Service Now service with these new settings	Service Now Admin Settings	Enabled if you have administrator privileges	Saves settings that were modified.

Table 11: Global Settings Command Buttons (*continued*)

Button Name	Description	Privileges	Enabled/Disabled	Results
Test Connection	<ul style="list-style-type: none"> In standard or partner-proxy modes, verifies the organization's connectivity with JSS In end-customer mode, verifies the organization's connectivity with the partner's Service Now application 	Service Now Admin Settings	Enabled if you have administrator privileges	Displays the Connection Status as Success or Failed.
Cancel	Withdraws the submission of modified settings	Service Now Admin Settings	–	Navigates back to the Global Settings page without saving the entries.

- Related Documentation**
- [Service Now Modes on page 19](#)
 - [Organizations Overview on page 41](#)
 - [Adding an SNMP Server on page 94](#)
 - [Editing and Deleting an SNMP Server on page 96](#)
 - [Configuring Proxy Server Settings on page 96](#)

Adding an SNMP Server

You can specify a destination for SNMP traps to be sent when a Service Now notification policy is triggered. SNMP traps are sent to these destinations only when the notification policy specifies this action. In **Service Now > Administration > Global Settings > SNMP Configuration**, the specified trap destinations are displayed.

To add and manage SNMP servers, you must have Service Now administration privileges.

To add an SNMP server:

1. From the Service Now taskbar, select **Administration > Global Settings > SNMP Configuration**.

The SNMP Servers page appears.

2. Click **Add**.

The **Add SNMP Server** dialog box appears.

3. Enter a name for the SNMP server, using alphanumeric values.
4. In the **SNMP Server** field, enter the SNMP server that is the IP address or hostname of the network management station where Service Now SNMP traps are sent. Do not use special characters.
5. Enter the UDP port number.
The User Datagram Protocol (UDP) port is a mechanism whereby a computer can simultaneously support multiple communication sessions with other computers and programs on the network. A port directs the request to a particular service that can be found at that IP address. The default UDP Port number is 162.
6. Enter a community string using only alphanumeric characters.
A community string is a password that allows access to a network device. It defines the community of people that can access the SNMP information on the device.
7. Select the protocol version from the list that specifies the SNMP versions.
8. Click **Add**.

The specified SNMP server is added to the Service Now database.

Loading MIBs

When using an MIB browser or other SNMP trap receivers such as HP OpenView to monitor the devices with SNMP, the following MIB files must be loaded. The **jnx-smi.mib** file must be loaded first:

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

Related Documentation

- [Configuring Global Settings on page 91](#)
- [Editing and Deleting an SNMP Server on page 96](#)
- [Configuring Proxy Server Settings on page 96](#)

Editing and Deleting an SNMP Server

SNMP servers are the destination for SNMP traps to be sent when a Service Now notification policy is triggered. You can modify the parameters of these SNMP servers and also delete them.

Editing an SNMP Server

To edit an SNMP server:

1. From the Service Now taskbar, select **Administration > Global Settings > SNMP Configuration**.

The SNMP Servers page appears.

2. Select the SNMP server whose parameters you want to modify.
3. Click **Edit**.
The **Edit SNMP** dialog box appears.
4. Make the desired changes to the parameters.
5. Click **Save**.

The changes are saved in the Service Now database. To verify, you can view the changes on the SNMP Servers page.

Deleting an SNMP Server

To delete an SNMP server:

1. From the Service Now taskbar, select **Administration > Global Settings > SNMP Configuration**.

The SNMP Servers page appears.

2. Select the SNMP server that you want to delete.
3. Click **Delete**.

The selected SNMP server is deleted from the Service Now database and is no longer displayed on the SNMP Servers page.

Related Documentation

- [Configuring Global Settings on page 91](#)
- [Adding an SNMP Server on page 94](#)
- [Configuring Proxy Server Settings on page 96](#)

Configuring Proxy Server Settings

You can configure Service Now to work with a proxy server. When you connect to a proxy server, all communication to and from JSS happens through the proxy server. Both SOCKS and HTTP proxies are supported in Service Now.

The proxy server evaluates the request according to the filters specified. For example, it may filter traffic by IP address or protocol. When the request is validated, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

To configure the proxy server settings:

1. From the Service Now taskbar, select **Administration > Global Settings > Proxy Server Configuration**.

The **Proxy Server Configuration** dialog box appears.

2. Enter the proxy address as a valid IP address or a valid hostname.
3. Specify the port on which the proxy server communicates with JSS. The default port number is 1080.
4. Enter the login username for authentication.
5. Enter the password that the identified user can use to log in.
6. Click **Submit**.

The proxy server settings are saved in the Service Now database.

**Related
Documentation**

- [Configuring Global Settings on page 91](#)
- [Adding an SNMP Server on page 94](#)
- [Editing and Deleting an SNMP Server on page 96](#)

CHAPTER 15

Auto Submit Policy

- [Auto Submit Policy Overview on page 99](#)
- [Creating an Auto Submit Policy on page 100](#)
- [Modifying an Auto Submit Policy on page 103](#)
- [Deleting Auto Submit Policies on page 104](#)
- [Exporting Incidents Report on page 104](#)
- [Changing the Status of Auto Submit Policies on page 105](#)

Auto Submit Policy Overview

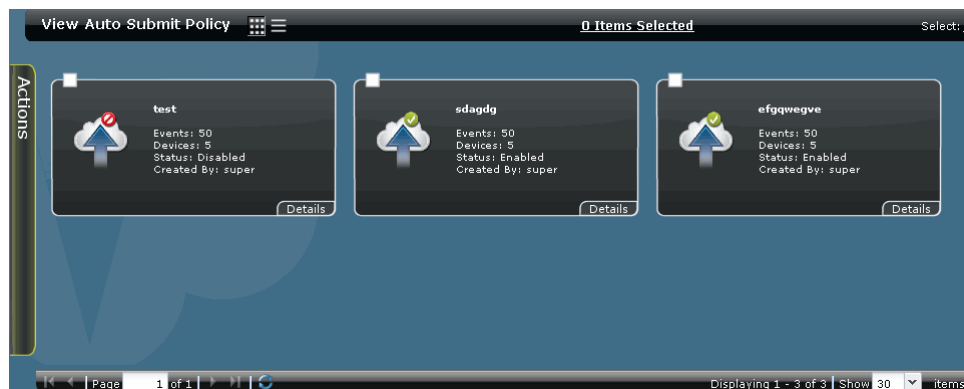
An auto submit policy is a policy that you create to enable Service Now to submit incidents to Juniper Support Services (JSS) automatically. While using Service Now in end-customer mode, auto submit policies allow Service Now to submit incidents automatically to the Service Now that it connects to. When incidents are submitted to JSS, technical support cases are created with Juniper Networks and the status of the incidents are updated on the Manage Incidents page in Service Now. When incidents are submitted automatically, they are filtered based on the JMB Filter Level setting of the Service Now organization to which the device belongs. These cases can be created from the **Manage Incidents** and the Create Auto Submit Policy pages.



NOTE: This option is not available when Service Now is in offline mode.

To view auto submit policies, select **Administration > Auto Submit Policy**, from the Service Now taskbar. The View Auto Submit Policy page appears as shown in [Figure 22 on page 100](#).

Figure 22: View Auto Submit Policy Page



You can perform the following tasks from the View Auto Submit Policy page

- Change the status of auto submit policies
- Export incidents report
- Delete auto submit policies
- Modify an auto submit policy [“Modifying an Auto Submit Policy” on page 103](#)

Related Documentation

- [Adding Devices to Auto Submit Policies on page 69](#)
- [Creating an Auto Submit Policy on page 100](#)
- [Adding an SNMP Server on page 94](#)
- [Creating and Editing a Notification Policy on page 132](#)

Creating an Auto Submit Policy

An auto submit policy enables incidents that occur on devices to be submitted to JSS automatically, creating a Tech Support Case. Although events with priority P1 can be included in auto submit policies, they do not get automatically submitted to JSS. Therefore, submit P1 events manually and call JTAC immediately.

To create an auto submit policy:

1. From the Service Now taskbar, select, **Administration > Auto Submit Policy > Create Auto Submit Policy**.

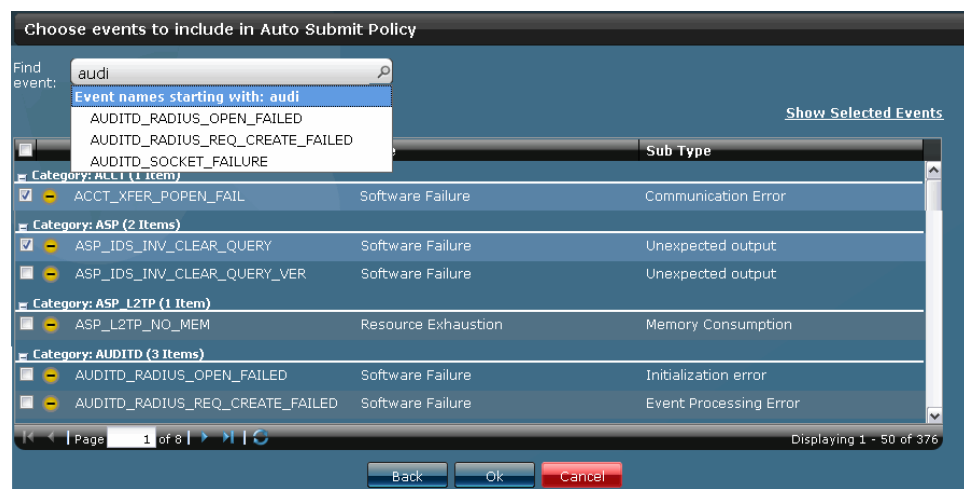
The Create Auto Submit Policy page appears as shown in [Figure 23 on page 101](#).

Figure 23: Auto Submit Policy Creation Page

Organization	Device Group	Hostname	Serial Number	Product	Version	Script Bundle
Gooma	DeviceGroup	Elmo	J1213	M7I	11.2B3	11.2R1.1
Gooma	DG	SRX-5600	JN11198B8AGB	SRX5600	11.1B1	Unavailable
Gooma	DG	nms3-f	A2831	M10I	10.2R1	Unavailable
Alcatel	AlcatelDG	ex-4200-50-182	BM0210435487	EX4200-24T	11.2B3	11.2R1.1
Alcatel	AlcatelDG	mx480-2-re0	JN11AFF42AFB	MX480	11.2B3	11.2R1.1
Gooma	DG	Device1111	F00000010011	MX960	9.5R2	
Gooma	DG	Device1117	F00000010017	MX960	9.5R2	
Gooma	DG	Device1115	F00000010015	MX960	9.5R2	
Gooma	DG	Device1120	F00000010020	MX960	9.5R2	

2. Enter a name for the policy. The name must begin with a letter having only alphanumeric (a-z, A-Z, 0-9), underscores (_), and hyphens (-).
3. Select the devices for which you want to create an auto submit policy.
To filter devices by their organizations or device groups, select the **Show** list, and select **By Organization** (as shown in [Figure 23 on page 101](#)) or **By Device Group**, respectively. A new list displays organizations or device groups.
4. (Optional) To display the list of selected devices that you want to include in the auto submit policy:
 - a. Click the **Show Selected Devices** link.
The **Selected Devices** dialog box displays the list of devices that you selected.
 - b. Verify the list and click **Close** to return to the Create Auto Submit Policy page.
5. Click **Next**.
The Choose events to include in Auto Submit Policy page appears.





Figure 24: Choose Events to Include in Auto Submit Policy Page



6. Select the events that you want to include in the auto submit policy. Events with priority P1 are not available for selection. Do not include events that are inactive for the selected devices. You can easily identify these events by looking at the icons that are used to represent them (see [Table 12 on page 102](#)).

To find events, type the event name in the **Find event** field and then select the event. As you type the event name, all event with event names that begin with the same alphabets are displayed in list. For example, as shown in [Figure 24 on page 102](#), when you type **audi** in the **Find event** field, all events with event names that begin with audi are displayed in a list.

Table 12: Icons That Represent the Event Types and Their Descriptions

Event Icons	Descriptions
	Event is inactive for all selected devices. Do not include this event in the event policy.
	Event is inactive for some selected devices.
	Event is active for all selected devices.
	Event is by default of priority P1 for one or more selected devices. Although these events can be included in the auto submit policies, they do not get automatically submitted to JSS. You can open a case for these events only by contacting customer care directly over phone.

7. (Optional) To display the list of selected events that you want to include in the auto submit policy:
 - a. Click the **Show Selected Events** link.
The **Selected Events** dialog box displays the events that you selected.
 - b. Verify the list and click **Close** to return to the Choose events to include in Auto Submit Policy page.
8. Click **OK**.
The **Results** dialog box lists the selected events and the devices on which they occurred.
9. Click **OK** to confirm.

The auto submit policy is created and the View Auto Submit Policy page appears. When the selected events occur on the devices that you specified, the events are automatically submitted to Juniper Support Services (JSS) and a Tech Support Case is created.
By default, auto submit policies are enabled. To disable auto submit policies, see [“Changing the Status of Auto Submit Policies” on page 105](#).
10. (Optional) To verify whether the auto submit policy is created with your specifications, navigate to the View Auto Submit Policy page and double click the auto submit policy to view its details.

Related Documentation

- [Adding an SNMP Server on page 94](#)
- [Creating and Editing a Notification Policy on page 132](#)
- [Administration Overview on page 39](#)
- [Adding Devices to Auto Submit Policies on page 69](#)

Modifying an Auto Submit Policy

Junos Space enables you to modify the events and devices that are specified in an auto submit policy.

To modify an auto submit policy:

1. From the Service Now taskbar, select, **Administration > Auto Submit Policy**.
The View Auto Submit Policy page appears.
2. Select the auto submit policy that you want to modify and select **Modify Auto Submit Policy** from either the **Actions** drawer or the right-click menu.

The details of the selected auto submit policy are displayed in an editable format.
3. Make your modifications to the events and devices for which the incidents must automatically be submitted to JSS.
4. Click **Save**.

Your changes are saved and the View Auto Submit Policy page appears.

5. (Optional) To verify your changes, double click the auto submit policy and view its details.

**Related
Documentation**

- [Adding an SNMP Server on page 94](#)
- [Creating and Editing a Notification Policy on page 132](#)
- [Adding Devices to Auto Submit Policies on page 69](#)

Deleting Auto Submit Policies

To delete auto submit policies:

1. From the Service Now taskbar, select, **Administration > Auto Submit Policy**.
The View Auto Submit Policy page appears.
2. Select the auto submit policies that you want to delete, and select **Delete** from either the **Actions** drawer or the right-click menu.
3. Click **Delete** again to confirm.

The selected auto submit policies are deleted and the View Auto Submit Policy page appears.

**Related
Documentation**

- [Auto Submit Policy Overview on page 99](#)
- [Creating an Auto Submit Policy on page 100](#)
- [Modifying an Auto Submit Policy on page 103](#)
- [Adding an SNMP Server on page 94](#)
- [Creating and Editing a Notification Policy on page 132](#)

Exporting Incidents Report

To export the information stored in auto submit policies:

1. From the Service Now taskbar, select, **Administration > Auto Submit Policy**.
The View Auto Submit Policy page appears.
2. Select the auto submit policies that you want to export into the Excel format, and select **Export** from either the **Actions** drawer or the right-click menu.
3. To open the Excel file, select **Open with** and click **Open**.
4. To save the Excel file on your local file system, select **Save File**, navigate to the folder where you want to save the Excel file, and click **OK**.
Detailed information about the selected auto submit policies appears in an Excel spread sheet.

- Related Documentation**
- [Modifying an Auto Submit Policy on page 103](#)
 - [Adding an SNMP Server on page 94](#)
 - [Creating and Editing a Notification Policy on page 132](#)

Changing the Status of Auto Submit Policies

To change the status of auto submit policies:



1. From the Service Now taskbar, select, **Administration > Auto Submit Policy**. The View Auto Submit Policies page appears.
2. Select the auto submit policies with status that needs to be changed from enabled to disabled, or vice versa, and select **Enable/Disable** from either the **Actions** drawer or the right-click menu.

The **Enable/Disable Auto Submit Policy** dialog box displays the current status of the selected auto submit policies.

3. Click **Submit**.
The action is initiated and a Jobs dialog box displays the Job ID which is also the link that takes you to the Manage Jobs page where you can view the status of this action.
4. Click **OK**.

The View Auto Submit Policy page (thumbnail view) represents auto submit policies using the icons listed in [Table 13 on page 105](#).

Table 13: Auto Submit Policy Icons

Icon	Description
	The auto submit policy is disabled.
	The auto submit policy is enabled.

- Related Documentation**
- [Modifying an Auto Submit Policy on page 103](#)
 - [Adding an SNMP Server on page 94](#)
 - [Auto Submit Policy Overview on page 99](#)
 - [Creating an Auto Submit Policy on page 100](#)
 - [Creating and Editing a Notification Policy on page 132](#)

PART 4

Service Central

- [Service Central Overview on page 107](#)
- [Incidents on page 109](#)
- [Information on page 121](#)
- [JMB Errors on page 129](#)
- [Notifications on page 131](#)

Service Central Overview

The Service Central workspace enables you to manage incidents, information messages, device snapshots, notifications, and error JMBs. Incidents are problem events that are detected in a device and sent to the Service Now application. When an event occurs on a device, the scripts installed on the device create files called Juniper Message Bundles (JMBs) that contain comprehensive information about the device identity, the problem event, and diagnostics. The JMB file is then transferred securely from the device to Service Now. Service Now searches for new incidents and displays the incidents on the Manage Incidents page within Service Central.

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

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

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

You can use a notification policy to specify the events for which you want to receive a notification. The options are New Incident Detected, Case Submitted, Case Status Updated, and Intelligence Update Received. Notification policies define other characteristics (filters) that you can use to fine tune the conditions under which you

receive a notification. You can even define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

Some tasks 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 end-customer mode is activated. For more information about the Service Now modes, see [“Service Now Modes” on page 19](#).

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

Using Service Central you can perform the following tasks:

- Assign an incident owner, notify users of an incident, update the status of incidents, and delete incidents.
- View and delete iJMBs, and export device data into HTML format.
- Assign messages to end-customers (enabled if you are a Service Now partner).
- Update end-customer cases (enabled if you are a Service Now partner).
- View, download, and delete JMBs with errors.
- View Knowledge Base articles associated with incidents.
- View information about devices that risk the chance of exposure.
- Generate JMBs on demand.
- Assign an owner, flag to users, and delete an information message.
- Create, edit, and delete a notification policy.

**Related
Documentation**

- [Service Now Overview on page 3](#)
- [Service Now Modes on page 19](#)
- [Incidents Overview on page 109](#)
- [Device Snapshots Overview on page 125](#)
- [Messages Overview on page 121](#)
- [JMB Errors on page 129](#)
- [Notification Policies Overview on page 131](#)

CHAPTER 16

Incidents

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Deleting an Incident on page 115](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Incidents Overview

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

A JMB file is an XML file that contains diagnostic information about the device and other information specific to the condition that triggered the event message. The incident contains information such as hostname, time stamp of the incident, synopsis, description, chassis serial number of the device, and the severity and priority of the incident.

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

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

incidents with various icons. These icons indicate incident priority levels and also whether the incidents are submitted to JSS. See “[Service Now Icons](#)” on page 27.

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

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

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

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

- Submit an incident to create a JTAC case
- Flag the incident to another user
- Assign the incident to another user
- Delete an incident
- View the details of a Juniper Message Bundle (JMB)
- View a Knowledge Base (KB) article pertaining to the incident
- View a case in the Juniper Networks Case Manager
- Remove a flag from the incident
- Add an e-mail address to the mailing list of an incident
- View technical support cases



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). As a workaround, see http://www.juniper.net/techpubs/en_US/junos9.5/information-products/topic-collections/swconfig-system-basics/time-zone-custom-configuring.html for information on how to configure a custom time zone.

Related Documentation

- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)

- [Deleting an Incident on page 115](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Assigning an Incident Owner

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

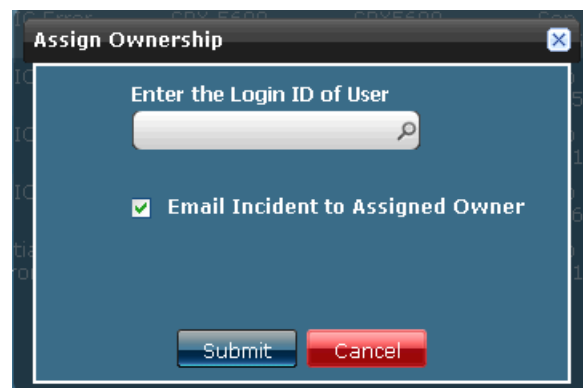
To assign an incident to a Service Now user:

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

The Manage Incidents page appears.

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

The **Assign Ownership** dialog box appears.



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

The incident is assigned to the specified user. See [“Viewing Device Snapshot Details” on page 128](#).

- Related Documentation**
- [Incidents Overview on page 109](#)
 - [Flagging an Incident to a User on page 112](#)
 - [Deleting an Incident on page 115](#)
 - [Checking Incident Status Updates on page 113](#)
 - [Exporting Incident Data on page 114](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
 - [Submitting an Incident to Juniper Support Systems on page 115](#)
 - [Viewing Incident Details on page 117](#)
 - [Viewing a Case in the Case Manager on page 118](#)
 - [Updating an End-Customer Case on page 119](#)

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 taskbar, select **Service Central > Incidents**.
The Manage Incidents table appears.
2. Select the incident that you want to flag to a user, and select **Flag to Users** from either the **Actions** drawer or the right-click menu.
The **Flag to Users** dialog box 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 newly flagged users of the incident. This option is selected by default.
5. Click **Submit**. The incident is flagged to the selected users.

- Related Documentation**
- [Incidents Overview on page 109](#)
 - [Assigning an Incident Owner on page 111](#)
 - [Deleting an Incident on page 115](#)
 - [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
 - [Checking Incident Status Updates on page 113](#)
 - [Exporting Incident Data on page 114](#)
 - [Submitting an Incident to Juniper Support Systems on page 115](#)
 - [Viewing Incident Details on page 117](#)

- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Checking Incident Status Updates

In Service Now, incidents are problem events that are detected in a device. Information about these incidents is sent to the Service Now application. Service Now routinely checks for new incidents. The Service Now **Manage Incidents** page provides a user interface to view incidents chronologically by organization name and device group.

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

Service Now provides three ways to check incident status.

- Using Junos Space logs. The Junos Space log of an incident displays a list of the status changes.
- Using notification policies. You can create a notification policy to notify users whenever the status of an incident is updated. For more information about creating notification policies, see [“Creating and Editing a Notification Policy” on page 132](#).
- Using the Service Central page. The My Incidents graph on the Service Central page displays the number of incidents whose status has changed since you last logged in. It also displays other information such as the number of incidents that were flagged to you, the number of incidents that you own, and the number of new incidents that were added since your last login. To view the Service Central page, select **Service Central** from the Service Now taskbar.

Related Documentation

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
- [Deleting an Incident on page 115](#)
- [Exporting Incident Data on page 114](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Exporting Incident Data

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

Exporting Incident Data into HTML

To export incident data into HTML format:

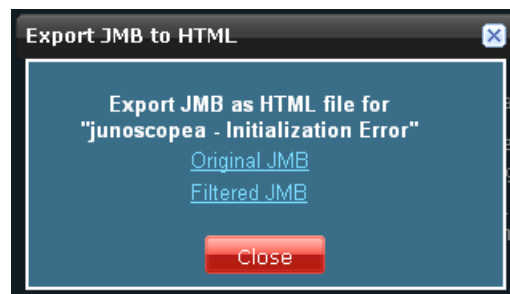
1. From the Service Now taskbar, select **Service Central > Incidents**.

The Manage Incidents page appears.

2. Select the device whose incident details you want to export.
3. Select **Export JMB to HTML** from the Actions drawer.

The **Export JMB to HTML** dialog box displays links to the original and filtered JMBs, as shown in [Figure 25 on page 114](#).

Figure 25: Export JMB to HTML Dialog Box



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

Exporting Incident Data into Excel

To export JMB data into Excel file format:

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

The Manage Incidents page appears.

2. Select the incident whose details you want to export.
3. Select **Export Incident Summary to Excel** from either the **Actions** drawer or the right-click menu.

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

4. Click the displayed link to save the incidents in Excel format

Related Documentation

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Deleting an Incident on page 115](#)

- [Checking Incident Status Updates on page 113](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Deleting an Incident

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

To delete an incident:

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

The Incidents table appears.

2. Select the incident that you want to delete.
3. Click **Delete**.

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

Related Documentation

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Submitting an Incident to Juniper Support Systems

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

in the Manage Incidents page. After you submit the incident, the status is **Submitted**. When the case is created by JSS, the status changes to **Created** and the Case ID appears.

To submit an incident:

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

The Manage Incidents page appears.

2. Select the incident for which you want to create a case, and select **Submit Case** from either the **Actions** drawer or the right-click menu.

The **Submit Case** dialog box displays the device name and incident synopsis.

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

3. Click the **Enter Email Id** field to enter an e-mail ID, and enter the e-mail ID in the format user@example.com.

To add multiple e-mail IDs, or delete them, use the **Add Email** and **Delete** buttons, respectively.

4. Click **Modify** to modify the site ID or username. The **Make Selection to Change Site ID or User** dialog box appears.

To modify the site ID, select the **Site ID** check box, and select the site ID from the **Site ID** list.

To modify the username, select the **User Name** check box, and enter the username and password in their respective fields. After your user credentials are validated, click **Get Sites** to select a site ID specific to the new user.

5. Select the method that you would like to use to 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**.
6. Enter the a customer tracking number in the **Customer Tracking Number** field.



NOTE: Steps 3 to 6 are applicable only for when your run Service Now in partner-proxy or standalone modes.

7. Select the priority of the case from the **Priority** list. The available options are Critical, High, Medium, and Low. The default priority is medium.
8. Enter your comments about the problem synopsis and a description of the case in the **Add Comments to Synopsis** and **Add Comments to Description** fields, respectively. Ensure that your comments are less than 1,028 characters.
9. Click **Save** to save your settings in the Service Now database and go back to the Manage Incidents page.
10. Click **Submit** to save your settings in the Service Now database and submit the selected incident to JSS.

The Manage Incidents page appears.

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

**Related
Documentation**

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Deleting an Incident on page 115](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Viewing Incident Details on page 117](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Viewing Incident Details

When incidents are received, only selected information appears on the Manage Incidents page. Using Service Now, you can view the entire content of the incident.

To view incident details:

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

The Manage Incidents page appears.

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

The **View JMB** dialog box displays links to the original and filtered JMB details.

3. Click the link to see the details of the selected incident.

**Related
Documentation**

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Deleting an Incident on page 115](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Viewing Knowledge Base Articles Associated with an Incident on page 118](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing a Case in the Case Manager on page 118](#)

- [Updating an End-Customer Case on page 119](#)

Viewing Knowledge Base Articles Associated with an Incident

Using Service Now you can view Knowledge Base (KB) articles associated with an incident.

To view the KB article associated with an incident:

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

The Manage Incidents table appears.

2. Select an incident to view the KB article associated with it, and select **View KB** from either the **Actions** drawer or the right-click menu.

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



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

Related Documentation

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Deleting an Incident on page 115](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Viewing a Case in the Case Manager on page 118](#)
- [Updating an End-Customer Case on page 119](#)

Viewing a Case in the Case Manager

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



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

To view a case in the Case Manager:

1. From the Service Now taskbar, select **Service Central > Incidents**.
The Manage Incidents page appears.
2. Select the incident whose details you want to view in the Case Manager, and select **View Case in Case Manager** from either the **Actions** drawer or the right-click menu.
The Juniper Networks Login page appears.



NOTE: If the **View Case in Case Manager** link is not enabled, ensure that the case has been created.

3. Enter your username and password and click **Login**.
The JSS Case Manager displays the case details.



NOTE: You can also view the details of the submitted cases in the Case Manager from the View Tech Support Cases page. To view case details, go to **Service Central > Incidents > View Tech Support Cases** and follow steps in “[Step-by-Step Procedure](#)” on page 119.

Related Documentation

- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Deleting an Incident on page 115](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Updating an End-Customer Case on page 119](#)

Updating an End-Customer Case

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



NOTE: This action is enabled only when Service Now operates in partner-proxy mode and when the state of the selected case is open.

To update an end-customer case:

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

The Manage Incidents page displays the list of incidents.

2. Select the end-customer incident for which you want to create a case, and select **End-Customer Case** from either the **Actions** drawer or the right-click menu.

The **End-Customer Case** dialog box appears as shown in [Figure 26 on page 120](#).

Figure 26: End-Customer Cases Dialog Box

End Customer Cases

Case ID: 124

Case Link: test

Case Status: Updated

Synopsis: CHASSISD_FASIC_PIO_READ_ERROR

Problem Description: The indicated routine failed with a read error at the indicated address and register for the indicated F chip and link on the indicated Control Board (CB): Fchip (CB test CB slot 01 ID fchip 01): read error in

Submit Cancel

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

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

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

Related Documentation

- [Service Now Overview on page 3](#)
- [Adding a Connected Member on page 46](#)
- [Incidents Overview on page 109](#)
- [Assigning an Incident Owner on page 111](#)
- [Flagging an Incident to a User on page 112](#)
- [Deleting an Incident on page 115](#)
- [Checking Incident Status Updates on page 113](#)
- [Exporting Incident Data on page 114](#)
- [Submitting an Incident to Juniper Support Systems on page 115](#)
- [Viewing Incident Details on page 117](#)
- [Viewing a Case in the Case Manager on page 118](#)

CHAPTER 17

Information

- [Messages Overview on page 121](#)
- [Assigning Ownership on page 122](#)
- [Flagging a Message to Users on page 122](#)
- [Deleting a Message on page 123](#)
- [Scanning a Message for Impact on page 124](#)
- [Assigning a Message to a Connected Member on page 124](#)
- [Device Snapshots Overview on page 125](#)
- [Exporting Device Data into HTML on page 127](#)
- [Deleting Device Snapshots on page 127](#)
- [Viewing Device Snapshot Details on page 128](#)

Messages Overview

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

You perform the following tasks using the Information Messages tab:

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

Related Documentation

- [Device Snapshots Overview on page 125](#)
- [Assigning Ownership on page 122](#)
- [Flagging a Message to Users on page 122](#)
- [Scanning a Message for Impact on page 124](#)

- [Deleting a Message on page 123](#)

Assigning Ownership

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

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

1. From the Service Now taskbar, select **Service Central > Information > Messages**.
The Manage Messages page appears.
2. Select the information message to which you want to assign an owner, and select **Assign Ownership** from either the **Actions** drawer 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 all the newly 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 122](#)
- [Scanning a Message for Impact on page 124](#)
- [Deleting a Message on page 123](#)
- [Assigning a Message to a Connected Member on page 124](#)
- [Viewing Messages Assigned to a Connected Member on page 49](#)
- [Messages Overview on page 121](#)
- [Device Snapshots Overview on page 125](#)

Flagging a Message to Users

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

To flag an information message to a user:

1. From the Service Now taskbar, 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** drawer 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 newly flagged users of the message. This option is selected by default.
5. Click **Submit**.

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

Related Documentation

- [Device Snapshots Overview on page 125](#)
- [Assigning Ownership on page 122](#)
- [Flagging a Message to Users on page 122](#)
- [Scanning a Message for Impact on page 124](#)
- [Deleting a Message on page 123](#)
- [Assigning a Message to a Connected Member on page 124](#)
- [Viewing Messages Assigned to a Connected Member on page 49](#)
- [Messages Overview on page 121](#)

Deleting a Message

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

To delete an information message:

1. From the Service Now taskbar, select **Service Central > Information > Messages**.
The Manage Messages page appears.
2. Select the information message that you want to delete, and select **Delete** from either the **Actions** drawer or the right-click menu.
3. Click **Delete** again to confirm the deletion.

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

Related Documentation

- [Device Snapshots Overview on page 125](#)
- [Assigning Ownership on page 122](#)
- [Flagging a Message to Users on page 122](#)
- [Scanning a Message for Impact on page 124](#)
- [Assigning a Message to a Connected Member on page 124](#)
- [Viewing Messages Assigned to a Connected Member on page 49](#)
- [Messages Overview on page 121](#)

Scanning a Message for Impact

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

To scan iJMBs and view the impacted devices:

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

The Manage Messages page appears.

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

The Scan for Impact Results page displays the list of devices that are impacted by the selected message. If no devices are impacted by the selected message, the following message appears:

No impacted devices found.

Related Documentation

- [Device Snapshots Overview on page 125](#)
- [Assigning Ownership on page 122](#)
- [Flagging a Message to Users on page 122](#)
- [Deleting a Message on page 123](#)
- [Assigning a Message to a Connected Member on page 124](#)
- [Viewing Messages Assigned to a Connected Member on page 49](#)
- [Messages Overview on page 121](#)

Assigning a Message to a Connected Member

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



NOTE: This action is available only when Service Now operates in partner-proxy mode. For more information about standard, partner-proxy, and end-customer modes, see [“Service Now Modes” on page 19](#).

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

To assign a message to a connected member:

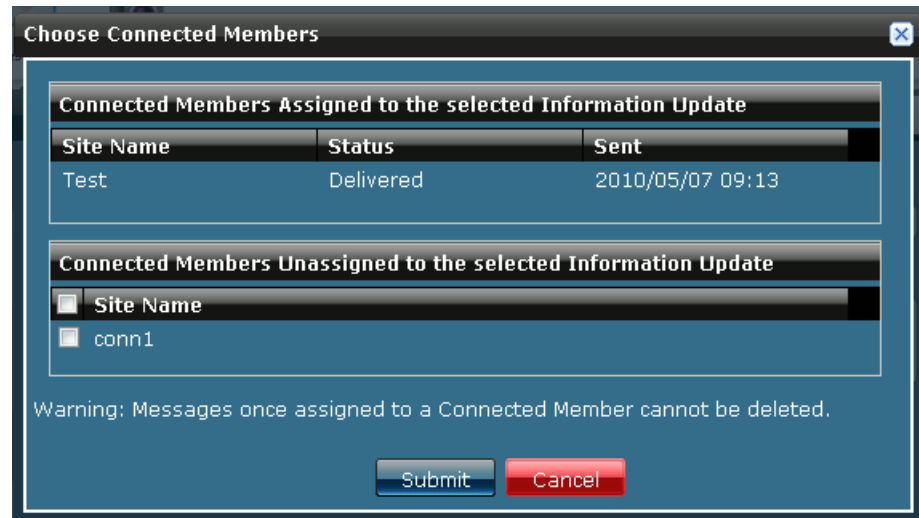
1. From the Service Now taskbar, select **Service Central > Information > Messages**.

The Manage Messages page displays the list of information messages received.

2. Select the message that you want to assign to a connected member, and select **Assign Message to End-Customer** from either the **Actions** drawer or the right-click menu.

As shown in [Figure 27 on page 125](#), the **Choose Connected Members** dialog box displays the list of connected members. It also the connected members to whom the message is already assigned along with the status (if any).

Figure 27: Choose Connected Members Dialog Box



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

The selected message is assigned to the connected member. To verify this action you can navigate to the Manage Organizations page, and list the messages assigned to any connected member. See [“Viewing Messages Assigned to a Connected Member” on page 49](#).

Related Documentation

- [Adding a Connected Member on page 46](#)
- [Device Snapshots Overview on page 125](#)
- [Assigning Ownership on page 122](#)
- [Flagging a Message to Users on page 122](#)
- [Scanning a Message for Impact on page 124](#)
- [Deleting a Message on page 123](#)
- [Viewing Messages Assigned to a Connected Member on page 49](#)
- [Messages Overview on page 121](#)

Device Snapshots Overview

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

to the Customer Intelligence Database (CIDB) database and then processed and analyzed to provide preventive measures.

You can filter the configuration content from device snapshots that are sent to JSS by setting the JMB Filter Level during organization creation (See [“Adding an Organization” on page 43](#)) and then track the status of the device snapshot submission to JSS. You can also stop device snapshots from being sent to JSS.

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

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

Devices that have stopped sending information (device snapshots) to Service Now for more than two weeks are also detected and graphically displayed on the Administration page. To list these devices you can click the Devices Not Sending Snapshots bar of the Devices Not Sending Device Snapshots graph. These devices are displayed on the Service Now Devices page where you can view their details and export them to HTML format. The thumbnail view of the Manage Device Snapshots page uses different icons to help you identify snapshots that have been successfully uploaded to JSS and the device snapshots whose submission to JSS failed. For a description of these icons, see [“Service Now Icons” on page 27](#).

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

- Exporting device data in HTML format
- Deleting a device snapshot
- Viewing device snapshot Details

Related Documentation

- [Exporting Device Data into HTML on page 127](#)
- [Deleting Device Snapshots on page 127](#)
- [Viewing Device Snapshot Details on page 128](#)
- [Messages Overview on page 121](#)

Exporting Device Data into HTML

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

To export device data in HTML format:

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

The Manage Device Snapshots page displays the device snapshots received.

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

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

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

Related Documentation

- [Device Snapshots Overview on page 125](#)
- [Deleting Device Snapshots on page 127](#)
- [Viewing Device Snapshot Details on page 128](#)
- [Messages Overview on page 121](#)

Deleting Device Snapshots

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

To delete an iJMB:

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

The Manage Device Snapshots page appears.

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

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

Related Documentation

- [Device Snapshots Overview on page 125](#)
- [Exporting Device Data into HTML on page 127](#)
- [Viewing Device Snapshot Details on page 128](#)
- [Messages Overview on page 121](#)

Viewing Device Snapshot Details

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

To view the details of an iJMB:

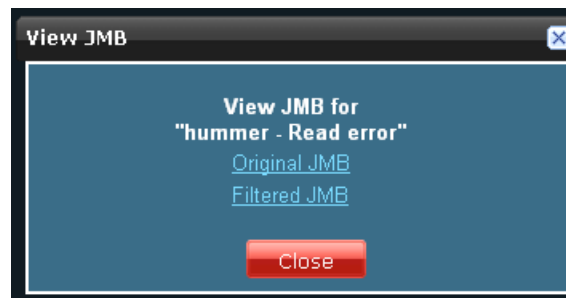
1. From the Service Now taskbar, select **Service Central > Information > Device Snapshots**.

The Manage Device Snapshots page appears.

2. Select the organization whose iJMB contents you want to view, and select **View JMB** from either the **Actions** drawer or the right-click menu.

The **View JMB** dialog box displays links to the original and the filtered iJMBs as shown in [Figure 28 on page 128](#). The information in the filtered JMB is classified by the settings on your Global Settings page.

Figure 28: View JMB Dialog Box



3. Click a link to view the iJMB details.

Related Documentation

- [Device Snapshots Overview on page 125](#)
- [Exporting Device Data into HTML on page 127](#)
- [Deleting Device Snapshots on page 127](#)
- [Messages Overview on page 121](#)

CHAPTER 18

JMB Errors

- [JMB Errors on page 129](#)

JMB Errors

JMBs with errors are Juniper Message Bundles (JMBs) that do not comply with the standard data structure or other data elements that Service Now accepts. Service Now identifies the JMBs with errors and displays them on the Manage 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 unique error JMBs.

- [Downloading JMB Errors on page 129](#)
- [Deleting JMB Errors on page 130](#)

Downloading JMB Errors

To download the JMB errors in a zipped file:

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

The Manage JMB Errors page appears.

2. Select the JMB whose details you want to download and select **Download JMB Errors** from either the **Actions** drawer or the right-click menu.

The **Download JMB Errors** dialog box appears.

Figure 29: Download JMB Errors Dialog Box



You can download up to five JMB files at a time.

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

Deleting JMB Errors

To delete an error JMB:

1. From the Service Now taskbar, select **Service Central > Incidents > JMB Errors**.
The Manage JMB Errors page appears.
2. Select the JMB that you want to delete, and select **Delete** from either the **Actions** drawer or the right-click menu.
The **Delete Error JMB** dialog box prompts you to confirm the deletion.
3. Click **Delete**.

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

- Related Documentation**
- [Service Central Overview on page 107](#)
 - [Messages Overview on page 121](#)

CHAPTER 19

Notifications

- [Notification Policies Overview on page 131](#)
- [Creating and Editing a Notification Policy on page 132](#)
- [Enabling or Disabling a Notification Policy on page 137](#)
- [Deleting a Notification Policy on page 138](#)

Notification Policies Overview

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

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

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

Service Now provides an interface where you can manage these notification policies. The Manage Notifications page displays the notification policies chronologically by name, owner, status, and trigger. For more information about the Manage Notifications table columns, see [Table 14 on page 131](#).

Table 14: Notification Policies Table Column Descriptions

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Name	Name of the policy which must be unique.	Hyperlink requires Notification Policy privilege	64 characters	—
Owner	Name of the user who owns the notification policy.	—	—	—

Table 14: Notification Policies Table Column Descriptions (*continued*)

Element Name	Description	Privilege Required to Modify	Range/Length	Default
Status	Whether the notification policy is running.	–	Enabled or Disabled	–
Trigger Type	Type of the trigger for which the notification policy is applied.	–	<ul style="list-style-type: none"> • New Incident Detected • Incident Submitted • Case ID Assigned • New Exposure • Service Contract Expiring • Case Status Updated • New Intelligence Update 	–

- Related Documentation**
- [Creating and Editing a Notification Policy on page 132](#)
 - [Enabling or Disabling a Notification Policy on page 137](#)
 - [Deleting a Notification Policy on page 138](#)

Creating and Editing a Notification Policy

Notification policies specify when you want Service Now to send notifications and the recipients. You can define the events that trigger the notification, the filters that further specify the trigger events, and the actions that you want Service Now to take after the event is triggered.

To create a notification policy:

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

The Create Notifications page appears.

Figure 30: Create Notifications Page

2. Enter a notification policy name, and select a trigger.
3. Enter the filter parameters.
Different filters are supported for incident and information trigger types.
4. Enter the e-mail IDs of users to whom the notification must be sent.
For more information about the fields in the **Create Notification Policy** dialog box, see [Table 15 on page 134](#).
5. Specify the destinations where SNMP traps can be sent when an event occurs in the **Send Traps to** section.
For more information about the fields in the **Create Notification Policy** dialog box, see [Table 15 on page 134](#).
6. Select the **Send JMB file as attachment in mail** check box if you want the owners of the notification to receive JMBs as e-mails.
7. Click **Add**.

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

Copying a Notification Policy

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



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

To copy a notification policy:

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

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

Editing a Notification Policy

To modify a notification policy:

1. From the Service Now taskbar, select **Service Central** > **Notifications** > **Create Notifications**.
The Create Notifications page appears.
2. Select the notification policy that you want to edit, and select **Edit filters and Actions** from either the **Actions** drawer or the right-click menu.
The Create Notifications page appears.
3. Edit the desired fields. For more information, see [Table 15 on page 134](#).

Table 15: Create Notification Policy Page Field Descriptions

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

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

Field	Description	Range/Length	Default
Trigger Type	Enter the type of trigger required to activate this policy. The fields in the filter table dynamically change according to the selected trigger type.	<ul style="list-style-type: none"> • New Incident Detected • Incident Submitted • Case ID Assigned • Case Status Updated • New Intelligence Update • Service Contract Expiring • New Exposure <p>NOTE: New Incident Detected is the only option available when Service Now is in offline mode.</p>	—

Apply Filters:**Filter Parameters for New Incident Detected, Incident Submitted, Case ID Assigned, and Case Status Updated Triggers:**

Priority	<p>Select a value in the Priority field.</p> <p>Service Now sends a notification if the priority of the incident matches the entered value. Regular expressions can also be used in this field.</p>	255 characters	Blank
Device Name	<p>Enter a value in the Device Name field.</p> <p>Service Now sends a notification if the name of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.</p>	255 characters	Blank
Serial Number	<p>Enter a value in the Serial Number field.</p> <p>Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.</p>	255 characters	Blank
Has the words	<p>Enter a value in the Has the words field.</p> <p>Service Now sends a notification if the specified words match any of the fields in the incident or the information message. Regular expressions can also be used in this field.</p>	255 characters	Blank
Does not have	<p>Enter a value in the Doesn't have field.</p> <p>Service Now sends a notification if the specified words do not match any of the fields in the incident or the information message. Regular expressions can also be used in this field.</p>	255 characters	Blank

Filter Parameters for New Intelligence Update Triggers:

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

Field	Description	Range/Length	Default
Intelligence Update Type	Enter a value in the Intelligence Update Type field. Service Now sends a notification if the type of information message update matches the entered value.	255 characters	Blank
Products Affected	Enter a value in the Products Affected field. Service Now sends a notification if the Products Affected field value in alert information messages matches the entered value	255 characters	Blank
Platform Type	Enter a value in the Platform Type field. Service Now sends a notification if the Platforms Affected field in alert information messages or the platform type field in information messages match the entered value	255 characters	Blank
Keywords	Enter a value in the Keywords field. Service Now sends a notification if the Keyword in information messages matches the entered value	255 characters	Blank
Serial Number	Enter a value in the Serial Number field. Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Software Version	Enter a value in the Software Version field. Service Now sends a notification if the software version in the information messages matches the entered value	255 characters	Blank
Devices Impacted	Enter a value in the Devices Impacted field. Service Now sends a notification if the devices impacted in the information messages matches the entered value	255 characters	Blank
Has the words	Enter a value in the Has the words field. Service Now sends a notification if the specified words match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Does not have	Enter a value in the Doesn't have field. Service Now sends a notification if the specified words do not match any of the fields in the incident or the information message. Regular expressions can also be used in this field.	255 characters	Blank
Filter Parameters for Service Contract Expiring Triggers:			
Device Name	Enter a value in the Device Name field. Service Now sends a notification if the name of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Serial Number	Enter a value in the Serial Number field. Service Now sends a notification if the serial number of the device the incident occurred on matches the entered value. Regular expressions can also be used in this field.	255 characters	Blank
Filter Parameters for New Exposure Triggers:			

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

Field	Description	Range/Length	Default
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. Regular expressions can also be used in this field.	255 characters	Blank
Actions:			
Send Email to	Specify the e-mail addresses of users who must receive an alert if the policy is triggered and matches the specified filter. To add a new e-mail address to the list, click Add Email . Click the Enter Email Id field to enter the e-mail address. The e-mail address should be in the format user@example.com. To delete an e-mail address from the list, select the e-mail address and click Delete .	65535 characters	Blank
Send Traps to	Specify the destinations where SNMP traps can be sent when an event occurs and matches the specified filter. See “Adding an SNMP Server” on page 94 .	—	—

- Related Documentation**
- [Notification Policies Overview on page 131](#)
 - [Enabling or Disabling a Notification Policy on page 137](#)
 - [Deleting a Notification Policy on page 138](#)

Enabling or Disabling a Notification Policy

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

To enable a notification policy:

1. From the Service Now taskbar, select **Service Central** > **Notifications**.
The Manage Notifications page appears.
2. Select the notification policies whose status you want to change, and select **Enable/Disable** from either the **Actions** drawer or the right-click menu.
The **Change Reaction Policy 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 changes from **Enabled** to **Disabled** or vice versa.

- Related Documentation**
- [Notification Policies Overview on page 131](#)
 - [Creating and Editing a Notification Policy on page 132](#)
 - [Deleting a Notification Policy on page 138](#)

Deleting a Notification Policy

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

To delete a notification policy:

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

The Manage Notifications page appears.

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

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

3. Click **Delete**.

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

- Related Documentation**
- [Notification Policies Overview on page 131](#)
 - [Creating and Editing a Notification Policy on page 132](#)
 - [Enabling or Disabling a Notification Policy on page 137](#)

PART 5

Index

- [Index on page 141](#)

Index

A

adding devices.....	58
AI-Script	
install.....	59
remove.....	63

C

conventions	
notice icons.....	xi
text.....	xi
customer support.....	xii
contacting JTAC.....	xii

D

dashboard overview	
Dashboard Gadgets.....	24
Service Now Workspaces.....	23
deleting	
device.....	67
device group.....	53
iJMB.....	127
incident.....	115
information message.....	123
notification policy.....	138
organization.....	48
device	
associate with device group.....	68
device group	
create.....	51
modify.....	52
documentation	
comments on.....	xii

E

end-customer mode.....	19
export device data	
CSV/Excel.....	63
export iJMB	
html.....	127
export inventory information	
CSV/Excel.....	64

G

generating on demand incidents.....	65
global settings	
global.....	91
proxy server.....	96
snmp server	
add	94
edit/delete.....	96

I

Icons.....	27
incident	
assigning owner.....	111
export to HTML/Excel.....	114
flagging.....	112
submitting.....	115
information message	
assign connected member.....	124
assign owner.....	122
flagging.....	122

J

JMB error.....	129
----------------	-----

M

manuals	
comments on.....	xii
mode.....	19

N

notice icons.....	xi
notification policy	
create.....	132
enable/disable.....	137

O

online, offline mode.....	19
organization	
add.....	43
modify.....	47
run in test mode.....	50
test connection to JSS.....	48
overview	
administration.....	39
AI-Scripts.....	85
device groups.....	51
device snapshots.....	125
devices.....	55
Incidents.....	109

messages.....	121
notifications.....	131
organization.....	41
Service Central	107

Q

quick start	
Service Now.....	7

S

scan iJMB for ipact.....	124
script bundle	
add.....	87
delete.....	88
Service Now Overview.....	3
support, technical See technical support	

T

technical support	
contacting JTAC.....	xii
text conventions defined.....	xi

U

user roles.....	31
-----------------	----

V

view	
case in Case Manager.....	118
iJMB details.....	128
incident details	117
viewing exposure.....	64