JUNIPER NETWORKS | Engineering Simplicity

Junos Space Service Now Administration

Published
2020-02-20

Release
18.1R1

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

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

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

Junos Space Service Now Administration
18.1R1
Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation | xi

Documentation and Release Notes | **xi**

Documentation Conventions | **xi**

Documentation Feedback | **xiv**

Requesting Technical Support | **xiv**

- Self-Help Online Tools and Resources | **xv**
- Creating a Service Request with JTAC | **xv**

1 **Automated Support and Prevention Overview**

Automated Support and Prevention Overview | 19

- Benefits of ASAP | **20**

AI-Scripts Overview | 21

- Working Modes of AI-Scripts | **22**
- Events Detected by AI-Scripts | **23**
- Types of JMBs | **23**
- JMB Contents | **24**
- Logs | **30**

2 **Service Now Administration Overview**

Service Now Administration Workspace Overview | 35

Service Now Modes | 36

- Service Now Modes Overview | **37**

Discovering Devices | 46

Juniper Networks Devices Supported by Service Now and Service Insight | 46

Service Now Domain Overview | 53

- Assigning a Service Now Object to Another Domain | **56**

3 Installing, Upgrading, and Uninstalling Junos Space Service Now

Installing Junos Space Service Now and Junos Space Service Insight Applications | 59

Uploading a Service Now and Service Insight Image File to a Junos Space Server | 59

Installing Junos Space Service Now and Junos Space Service Insight | 61

Upgrading Junos Space Service Now and Junos Space Service Insight Applications | 63

Uninstalling Junos Space Service Now and Junos Space Service Insight Applications | 65

4 Managing Global Settings

Service Now Global Settings Overview | 69

Associated Actionsk | 74

Configuring Global Settings | 75

Adding an SNMP Configuration to Service Now | 80

Editing an SNMP Configuration | 81

Managing SNMP Traps | 82

Viewing Proxy Server Settings Configured on the Junos Space Platform | 84

Configuring SFTP Server for Uploading Core Files Generated for Events | 84

Directive File Overview | 86

Updating the Directive File in Junos Space Service Now | 88

Restoring the Default Directive File | 91

Configuring Advanced Filter Settings | 92

5 User Roles

User Roles and Permissions Overview | 97

Junos Space Service Now User Roles | 97

Junos Space Service Insight User Roles | 103

6 Service Now End Customer-Partner Communication

Service Now End Customer–Partner Communication Overview | 107

- Generating CSR by Service Now Partner | 108
- Obtaining Signature of a Certificate Authority | 111
- Uploading the Certificate to Service Now Partner | 111
- Obtaining the Intermediate Certificate (key) for Establishing Credibility of the SSL Certificate | 111
- Obtaining SSL Certificate of the Service Now Partner | 112

Installing the SSL Certificate on a Service Now End Customer | 113

7 Configuring and Managing Organizations

Service Now Organizations Overview | 119

- Associated Actions | 121

Adding an Organization to Service Now | 122

Adding an End Customer to Service Now Configured in Partner Proxy Mode | 125

Modifying Organization Parameters | 128

Deleting an Organization | 129

Testing the Connection to JSS | 130

Running an Organization in Test Mode | 131

Updating Core File Upload Configuration for an End Customer | 132

Viewing Messages Assigned to an End Customer | 132

8 Configuring and Managing Device Groups

Service Now Device Groups Overview | 137

- Associated Actions | 137

Creating a Device Group | 138

Modifying a Device Group | 140

Deleting a Device Group | 142

9

Managing Service Now Devices

Service Now Devices Overview | 147

Associated Actions | 152

Adding Devices to Junos Space Service Now | 155

Installing an Event Profile on a Device by Using Service Now | 156

Manually Installing AI-Scripts on Devices | 160

Uninstalling an Event Profile from a Device | 165

Configuring AI-Scripts Parameters by Using Junos Space Service Now | 167

Deleting a Device from Junos Space Service Now | 170

Associating Devices with a Device Group | 171

Assigning an Auto Submit Policy to a Device | 172

Generating an On-Demand Incident | 174

Generating an On-Demand Device Snapshot | 180

Generating an RMA Incident for a Device | 182

Verifying the Connection Between a Device and the SFTP Server | 186

Collecting RSI and System Log Files | 187

Configuring BIOS Validation for Verifying BIOS Integrity of a Device | 191

Exporting Device Data in CSV and Excel Formats | 193

Exporting Inventory Information in CSV Format | 195

Viewing Incidents Created for a Device | 196

Viewing Exposure for a Device | 196

Moving a Device to Maintenance Mode | 198

10 Configuring and Managing Event Profiles and Script Bundles

Service Now Event Profiles Overview | 203

Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview | 205

Associated Actions | 209

Adding an Event Profile to Junos Space Service Now | 210

Cloning an Event Profile | 214

Importing Event Profiles into Junos Space Service Now in XML Format | 219

Deleting Event Profiles from Junos Space Service Now | 221

Pushing an Event Profile to Devices | 221

Setting an Event Profile as the Default Event Profile in Junos Space Service Now | 225

Adding a Script Bundle to Junos Space Service Now | 226

Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now | 227

Deleting a Script Bundle from Junos Space Service Now | 228

Displaying Devices Associated with an Event Profile | 229

Exporting Events Data in Excel Format | 229

Exporting Event Profiles from Junos Space Service Now in XML Format | 230

11 Configuring and Managing Auto Submit Policies

Service Now Auto Submit Policy Overview | 237

Associated Actions | 239

Creating an Auto Submit Policy | 239

Modifying an Auto Submit Policy | 245

Changing the Status of Auto Submit Policies | 247

Deleting Auto Submit Policies from Service Now | 248

Exporting an Incidents Report | 249

Changing the Dampening Status of an Auto Submit Policy | 250

12 Managing Incident Filters

Service Now Incident Filters Overview | 255

Associated Actions | 256

Viewing Incident Filters Configured on Junos Space Service Now | 257

Creating Incident Filters | 258

Creating a Basic Incident Filter | 259

Creating an Advanced Incident Filter | 261

Importing Incident Filters to Service Now | 263

Modifying an Incident Filter | 264

Exporting Incident Filters | 266

Reordering Incident Filters | 267

Enabling Incident Filters | 269

Disabling Incident Filters | 270

Deleting Incident Filters | 271

13 Managing Auto Submit Filters

Service Now Auto Submit Filters Overview | 275

Actions That You Can Perform From the Auto Submit Filters Task | 277

Creating Auto Submit Filters | 278

Creating a Basic Auto Submit Filter | 278

Creating an Advanced Auto Submit Filter | 280

Importing Auto Submit Filters to Service Now | 282

Modifying an Auto Submit Filter | 283

Exporting Auto Submit Filters | 286

Reordering Auto Submit Filters | 287

Enabling Auto Submit Filters | 289

Disabling Auto Submit Filters | 291

Deleting Auto Submit Filters | 292

14 Configuring and Managing Product Health Data Collection

Product Health Data Collection Configuration Overview | 297

Benefits of Product Health Data Collection | 299

Actions That You Can Perform From the Product Health Data Collection Task | 299

Configuring Product Health Data Collection on a Device | 300

Configuring PHDC by Using the Product Health Data Collection Task | 300

Configuring PHDC by Using the Service Now Devices Task | 303

Viewing Product Health Data Files Collected from a Device | 307

Modifying a Product Health Data Collection Configuration | 310

Rescheduling a Product Health Data Collection Configuration | 313

Retrying Collecting Product Health Data from a Device | 315

Disabling Product Health Data Collection on a Device | 316

Enabling Product Health Data Collection on a Device | 317

Aborting a Product Health Data Collection Configuration | 319

Exporting Product Health Data Information to an Excel File | 321

Exporting Information about Devices on which PHDC is configured | 322

Exporting Data about PHD Files Collected from a Device | 324

Deleting Product Health Data Files Collected from a Device | 327

Deleting a Product Health Data Collection Configuration from Service Now | 329

15 Configuring and Managing Address Groups

Service Now Address Group Overview | 333

Associated Actions | 333

Creating an Address Group | 334

Modifying an Address Group | 334

Deleting Address Groups | 335

Associating Devices with an Address Group From the Address Groups Page | 336

Associating Devices with an Address Group From the Organizations Page | 338

Associating Devices with an Address Group from the Device Groups Page | 340

Associating Devices with an Address Group from the Service Now Devices Page | 341

16 Managing E-mail Templates

Service Now E-Mail Templates Overview | 345

Associated Actions | 348

Viewing E-Mail Templates | 348

Modifying an E-Mail Template | 350

17 Appendix

Commands Used for Collecting PHD from Managed Devices | 353

| 353

Sample Perl Script for Incident and Auto Submit Filters | 357

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xi
- Documentation Conventions | xi
- Documentation Feedback | xiv
- Requesting Technical Support | xiv

Documentation and Release Notes

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

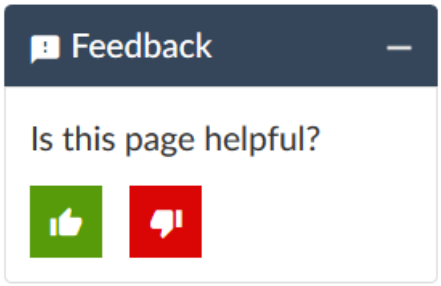
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

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



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

1

CHAPTER

Automated Support and Prevention Overview

Automated Support and Prevention Overview | **19**

AI-Scripts Overview | **21**

Automated Support and Prevention Overview

Juniper Networks Automated Support And Prevention (ASAP) is an end-to-end solution designed to automatically resolve product issues, prevent outages, provide insight and increase network productivity. With ASAP, a network operator can perform the following functions:

- Monitor faults.
- Collect diagnostic data.
- Manage events.
- Create cases for resolving issues.
- Manage inventory.
- Receive notifications from Juniper Support Systems (JSS) about issues that can affect the device.
- Receive End-of-Life (EOL) and End-of-Service (EOS) notifications from JSS for managed devices and device components.
- Create reports using the received notifications and analyze the impact of known issues on the network.

ASAP is provided to all customers with Juniper Care and Juniper Care Plus service contracts. ASAP comprises the following components:

- Advanced Insight-Scripts (AI-Scripts):

  AI-Scripts are XML, XSLT, or SLAX scripts installed on devices running Junos OS Release 11.4 or later to detect hardware and software events such as fan failure, read-write errors, routing protocol checksum error, critical packet drops, and failure to commit configurations. When an event occurs on a device on which AI-Scripts are installed, AI-Scripts are triggered to collect troubleshooting information from the device, which is bundled in a structured format called a Juniper Message Bundle (JMB).

  AI-Scripts generate three types of JMBs—eJMBs, iJMBs, and on-demand JMBs. Event JMBs or eJMBs are generated in response to events occurring on the device. Information JMBs or iJMBs (also known as device snapshots) are generated to provide trending information of a device. On-demand JMBs are generated in response to user requests to generate a JMB.

  For more information about AI-Scripts, see *AI-Scripts and JMBs Overview*.

- Junos Space Service Now and Junos Space Service Insight applications:
  - Service Now accesses the JMBs generated by AI-Scripts from devices running Junos OS, creates an incident for the event in the Service Now database, and notifies the network operator about the event. Service Now can be configured to submit the incident and the associated JMB to JSS automatically to create a case for resolving any issue caused by the event.

    You can use Service Now (instead of AI-Scripts) to generate a JMB in situations where you want to check the health of the device well before receiving an iJMB. This JMB is known as an off-box

on-demand iJMB. Service Now can also generate off-box on-demand eJMBs and off-box on-demand Return Materials Authorization (RMA) JMBs. Service Now uses the **directive.rc** file to generate the off-box JMBs. The **directive.rc** file is shipped with Service Now and contains the required commands to generate the JMBs.

For more information about the directive file, see "Directive File Overview" on page 86

- Service Insight stores alerts called proactive bug notifications (PBNs) received from JSS and notifies the network operator about impending problems in the network. Service Insight also stores alerts for devices and services nearing EOL, EOS, Last Order Date, or End of Engineering. Service Insight receives these alerts from JSS based on the trending information of iJMBs submitted by Service Now.

  You can generate an EOL and PBN report to identify the devices exposed to known issues or bugs and devices nearing EOL or EOS for taking suitable action to mitigate network downtime.

  For more information, see *Proactive Information Received from Juniper Support Systems (JSS)*.

- Juniper Support Systems (JSS):

  JSS comprises knowledge repositories, such as the EOL or EOS database, the Juniper Customer Relationship Manager (CRM), Juniper Contracts systems, and bugs database.

  JSS creates cases for incidents submitted by Service Now. The cases are assigned to JTAC personnel for resolution. Users are notified about the progress of the case through the Service Now GUI.

  JSS uses the information present in iJMBs to send alerts about devices and services nearing EOL agreements. While resolving an issue received from a customer, JSS analyzes the nature of the issue and sends PBNs to warn other customers about the issue to mitigate network downtime.

- Juniper Case Analysis Tool Suite (JCATS)

  JCATS is a set of tools that automatically analyze data collected and attached to cases opened in Juniper Networks case management systems and provide analysis results to JTAC engineers. JTAC engineers can use this data to speed up diagnosis and problem resolution.

Benefits of ASAP

- Allows network operators to automatically detect events on a device running Junos OS for early resolution of issues.
- Allows quick collection of necessary troubleshooting data without any manual intervention, thus saving time and effort.
- Provides critical information related to bugs, EOL, and EOS so that network operators and customers can plan to mitigate any adverse impact on their network.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Service Now Overview

Service Insight Overview

Installing Junos Space Service Now and Junos Space Service Insight Applications | 59

AI-Scripts Overview

IN THIS SECTION

- Working Modes of AI-Scripts | 22
- Events Detected by AI-Scripts | 23
- Types of JMBs | 23
- JMB Contents | 24
- Logs | 30

Advanced Insight Scripts (AI-Scripts) provide the intelligence that devices need to automatically detect and report hardware and software failure or other functional abnormalities to ensure maximum network uptime. AI-Scripts are imported into Service Now in the form of script bundles.

An AI-Scripts bundle contains event policies. An event policy defines the Junos OS commands that are executed to collect troubleshooting data when an event occurs on the device. One event policy is defined for each event. For information about adding a script bundle to Service Now, see "Adding a Script Bundle to Junos Space Service Now" on page 226.

When AI-Scripts are installed on a device, the device is said to be AI-Scripts-enabled. An AI-Scripts-enabled device can automatically detect events, such as failure to allocate memory for a process or failure of a hardware when it occurs, and report the event to the network operator. When an event occurs, AI-Scripts generates data about the event, packages the data in a structured format called a Juniper Message Bundle (JMB), and stores the JMB at a defined location on the device from where Junos Space Service Now accesses the data.

This section contains the following topics:

Working Modes of AI-Scripts

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

- Reactive mode: In reactive mode, the AI-Scripts collect data from the device when a predefined event, such as failure to allocate memory for a process or failure of a hardware, occurs on the device and store the data at a predefined location on the device from where Service Now accesses it for analysis and resolution. The JMB generated in this mode is known as an event JMB or eJMB.
- Proactive mode: In proactive mode, the AI-Scripts periodically collect data on vital system functions and store the data at a predefined location on the device. This data is accessed by Service Now to monitor the device and to predict and prevent risks related to the device. The JMB generated in this mode is known as an informational JMB or iJMB.

Apart from event and informational JMBs, AI-Scripts also generate JMBs in response to an event triggered by a user. These JMBs are known as on-demand incident JMBs. The on-demand JMBs can be of two types—on-box on-demand JMB or off-box on-demand JMB.

An on-box on-demand JMB is generated by AI-Scripts installed on the device in response to on-demand request by user. An off-box on-demand JMB is generated by Service Now by executing preconfigured commands on the device. You can use the off-box on-demand JMB to get information about a device when AI-Scripts are not installed on the device.

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 ASIC issues

For a complete list of events detected by AI-Scripts:

- for AI-Scripts Releases earlier than 6.0R1.0, refer to the latest version of *AI-Scripts Release Notes* at Service Automation Index Page
- for AI-Scripts Releases 6.0R1.0 and later, refer to the *AI-Scripts Feature Guide* at AI-Scripts Index page.

Types of JMBs

A Juniper Message Bundle (JMB) generated on a device running Junos OS can be of the following types:

- Event JMB or eJMB—JMB generated in response to events such as memory allocation error, read-write errors, or configuration commit failures that occur on devices

  An eJMB contains manifest, attachment, and log sections.

- Intelligence JMB or iJMB—JMB generated periodically to provide trend and health data of a device

  An iJMB contains manifest, trend data, and attachment sections.

- RMA JMB—JMB generated when a device component (for example, a fan) fails

  When a component fails, the relevant AI-Script in the AI-Scripts bundle is triggered to collect the required data for compiling the RMA JMB and reporting the event.

- On-demand JMBs—On-demand JMBs are generated when a user requests for a JMB to be generated on the device. On-demand JMBs can be of the following types:

  On-demand JMBs can be of the following types:

  - On-demand JMBs generated by AI-Scripts: AI-Scripts generate on-demand JMBs by using the **/var/db/scripts/on-demand.slax** script present in the AI-Scripts bundle. AI-Scripts can only generate on-demand eJMBs.
  - On-demand JMBs generated by Service Now: Service Now generates on-demand JMBs by using the **directive.rc** file packaged with Service Now. The **directive.rc** file contains the commands to generate JMBs.

    Service Now can generate the following types of JMBs:

- On-demand eJMB
- On-demand iJMB
- On-demand RMA JMB

JMB Contents

A JMB has the following structure:

- Manifest: The JMB manifest contains a summary of the information primarily needed for creating and submitting a case with JSS for an event. Elements displayed in the manifest section depend on the type of the JMB.

  Starting in Service Now Release 15.1R1, the Manifest section displays the following information: RSI Collection, BIOS Validation, Log Collection, Junos Software Version, Junos Space Version, Service Now Version, Product Health Data Collection, Product Health Data Collection Command File, JMB Cleanup Interval.

  Table 3 on page 24 lists the elements present in a JMB manifest.

  Table 3: Elements in the Manifest Section of a JMB

Element	Description
Event Information	
Host Event-ID	Specifies the ID of the event in response to which the JMB is generated Host Event-ID is represented in the following format: *<router-name>-<chassis-serial-number>-<YYYYMMDD-HHMMSS>-<sequence number>*, where: • *router-name* specifies the hostname of the router. • *chassis-serial-number* specifies the serial number of the router chassis. • *YYYYMMDD-HHMMSS* specifies the date and time the event occurred on the device. • *sequence number* varies from 001 through 999 and indicates the sequence of events when multiple events occur at the same time. The *sequence number* is present only if multiple events occur at the same instance on the device.

Table 3: Elements in the Manifest Section of a JMB *(continued)*

Element	Description
Problem Class	Specifies the problem class; the value is always set to Support. This field is used to populate the Problem Class field in the Customer Relationship Management System (CRM) of Juniper Support System (JSS). This field is not applicable for an iJMB.
Service Type	Specifies whether a JMB is generated as a proactive measure or a reactive measure. Possible values are: • Event: The JMB is generated in response to an event that occurred on the device. (This is a reactive measure.) • Intelligence: The JMB is generated and collected periodically to monitor the vital functions of the device. (This is a proactive measure.) • On-demand: The JMB is generated in response to a request from a user. • Event-RMA: The JMB Is generated in response to an Return Material Authorization (RMA) event on the device. This is a reactive measure. • Health-check: The JMB is generated and collected periodically to check the integrity of the BIOS or for any errors related to the AI-Scripts installed on the device. This is a proactive measure.
Time Occurred	Specifies the time at which the event occurred
Event Type Group	Classifies the events that occurred on the device under the following categories: • Hardware failure • Software failure • Resource exhaustion This field is not applicable for an iJMB.

Table 3: Elements in the Manifest Section of a JMB *(continued)*

Element	Description
Event Type	Specifies the type of event that occurred on the device; for example, MAC error or Process error This field is not applicable for an iJMB.
Problem Synopsis	Specifies a summary of the event; this field is used to populate the Problem Synopsis field in the CRM. This field can be appended with your text while submitting the incident for resolution to JSS or a Service Now partner. This field is not applicable for an iJMB.
Problem Description	Describes the event; this field is used to populate the Problem Description field in the CRM. This field can be appended with your text while submitting the incident for resolution. This field is not applicable for an iJMB.
Problem Severity	Specifies JTAC's assessment of the impact that the event has on the customer's network Possible values are: • 1 - Critical • 2 - High • 3 - Medium • 4 - Low This field is not applicable for an iJMB.

Table 3: Elements in the Manifest Section of a JMB *(continued)*

Element	Description
Problem Priority	Specifies the customer's perception of the impact that the event has on the network; this field is used to populate the Problem Priority field in the CRM system. Possible values are: • 1 - Critical • 2 - High • 3 - Medium • 4 - Low This field is not applicable for an iJMB.
KBURL	Specifies the link to the knowledge base (KB) article related to the event This field is not applicable for an iJMB.
AI-Script Version	Specifies the version of the AI-Scripts that generated the JMB
Associated Core File	Specifies the core files included in the JMB This field is not applicable for an iJMB.
Router Information	
Product Name	Specifies the name of the product; this field is used to populate the Platform field in CRM.
Host Name	Specifies the hostname assigned to the device
OS Platform	Specifies the routing OS installed on the device
Routing Engine	
Name	Specifies the name of the Routing Engine
Mastership State	Specifies whether the Routing Engine serves as the primary or the backup Routing Engine of the device
Component	Specifies the components of Junos OS such as rpd and chassid

Table 3: Elements in the Manifest Section of a JMB *(continued)*

Element	Description
Version	Version of Junos OS component executing on the Routing Engine
Builder	User who created the Junos OS build
Build Date	Date and time the Junos OS build was created
Service Now Information	
RSI Collection	Specifies the configuration for collecting Request Support Information (RSI) from the device—whether RSI collection is enabled or disabled and the interval for collecting RSI
BIOS Validation	Specifies whether BIOS validation is enabled or disabled on the device
Log Collection	Specifies whether log collection is enabled or disabled on the device True indicates that log collection is enabled and False indicates that log collection is disabled.
Space Platform Version	Specifies the version of Junos Space Network Management Platform managing the device
Service Insight	Specifies the version of Service Insight installed with Service Now
Service Now	Specifies the version of Service Now managing the device
AI-Scripts Information	
RSI Collection	Specifies the configuration for collecting Request Support Information (RSI) from the device—whether RSI collection is enabled or disabled and the interval for collecting RSI

Table 3: Elements in the Manifest Section of a JMB *(continued)*

Element	Description
Log Collection Enabled	Specifies whether log collection is enabled or disabled on the device True indicates that log collection is enabled and False indicates that log collection is disabled.
BIOS Validation	Specifies whether BIOS validation is enabled or disabled on the device
PHD Collection	Specifies whether collection of product health data (PHD) is enabled or disabled on the device
PHD Collection Commands File	Specifies the file that contains the commands to collect PHD on the device
JMB Cleanup Interval	Specifies the interval in seconds after which JMBs generated due to PHD collection are deleted

- Trend data: Trend data provide information about the hardware and software operating parameters such as CPU and memory utilization of the Routing Engine and traffic statistics of the Packet Forwarding Engine of the device.

  Trend data are provided for the following:

  - Routing Engine
  - Flexible PIC Concentrators
  - Packet Forwarding Engine
  - Switch Control Board (SCB)
  - Routing protocol process (RPD)
  - Kernel

- Attachment: The files and data in a JMB depend on the type of the event that triggered the JMB. This section provides the output of specific Junos OS commands executed to retrieve data and log files pertaining to the event. Some commands are standard—that is, they are executed for every platform. Some commands are executed specific to a platform. The following commands are common to all platforms:

  - **show system processes extensive**
  - **show pfe statistics error**
  - **show system boot-messages**

- **show system virtual-memory**
- **show system buffer**
- **show system queues**
- **show system statistics**
- **show task io**
- **show configuration**
- **show chassis hardware**

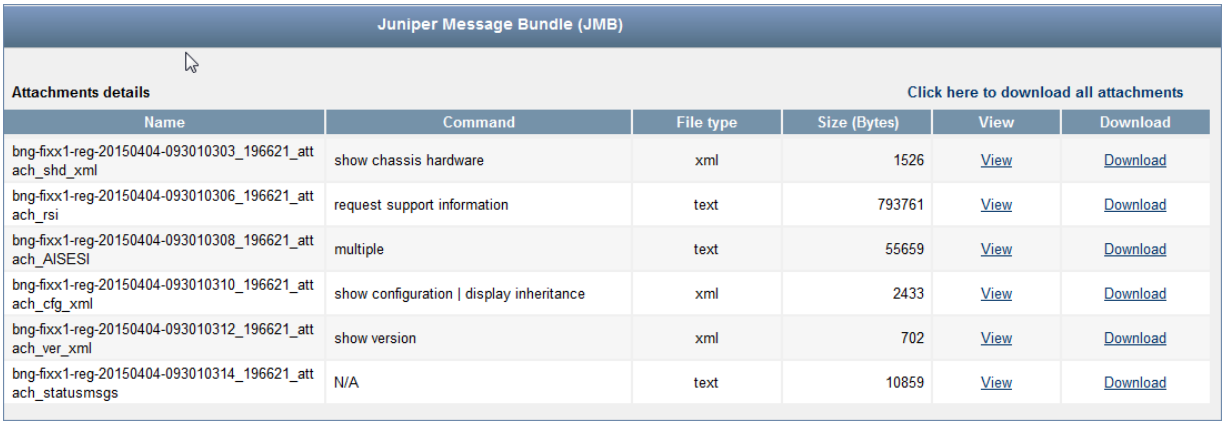
From Service Now Release 14.1R3 onwards, the attachments of an off-box on-demand JMB also include information about the last four configuration changes made on the device.

Starting in Service Now Release 15.1R2, the Attachments section displays the statuses of reading each attachment from the device and uploading each attachment file to JSS or Service Now partner.

The attachment files are retrieved from the device and stored in the Service Now database. The JMB contains links to view and download attachment files.

Figure 1 on page 30 shows the Attachment section of a JMB.

Figure 1: Attachment Section of a JMB



Juniper Message Bundle (JMB)

Attachments details — Click here to download all attachments

Name	Command	File type	Size (Bytes)	View	Download
bng-fixx1-reg-20150404-093010303_196621_attach_shd_xml	show chassis hardware	xml	1526	View	Download
bng-fixx1-reg-20150404-093010306_196621_attach_rsi	request support information	text	793761	View	Download
bng-fixx1-reg-20150404-093010308_196621_attach_AISESI	multiple	text	55659	View	Download
bng-fixx1-reg-20150404-093010310_196621_attach_cfg_xml	show configuration | display inheritance	xml	2433	View	Download
bng-fixx1-reg-20150404-093010312_196621_attach_ver_xml	show version	xml	702	View	Download
bng-fixx1-reg-20150404-093010314_196621_attach_statusmsgs	N/A	text	10859	View	Download

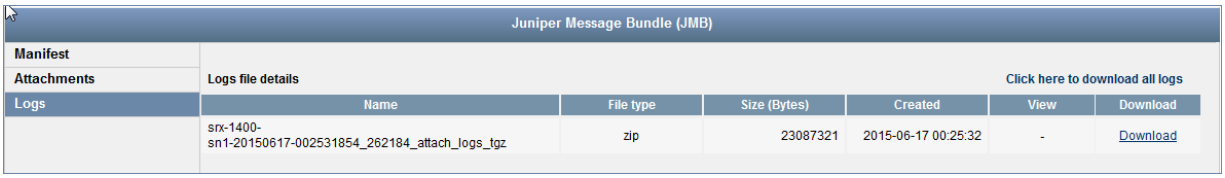
Logs

This section contains a compressed view of the **/var/log** directory of the device. However, if the **/var/tmp** directory has less than 20% of the required free space, the contents are collected in an attachment.

The log files are retrieved from the device and stored in the Service Now database. The JMB contains the links to view and download the log files.

Figure 2 on page 31 shows the log section of a JMB.

Figure 2: Log Section of a JMB



Release History Table

Release	Description
15.1R2	Starting in Service Now Release 15.1R2, the Attachments section displays the statuses of reading each attachment from the device and uploading each attachment file to JSS or Service Now partner.
15.1R1	Starting in Service Now Release 15.1R1, the Manifest section displays the following information: RSI Collection, BIOS Validation, Log Collection, Junos Software Version, Junos Space Version, Service Now Version, Product Health Data Collection, Product Health Data Collection Command File, JMB Cleanup Interval

RELATED DOCUMENTATION

Adding a Script Bundle to Junos Space Service Now | **226**

Deleting a Script Bundle from Junos Space Service Now | **228**

2

CHAPTER

Service Now Administration Overview

Service Now Administration Workspace Overview | 35

Service Now Modes | 36

Discovering Devices | 46

Juniper Networks Devices Supported by Service Now and Service Insight | 46

Service Now Domain Overview | 53

Service Now Administration Workspace Overview

Junos Space Service Now Administration workspace allows you to perform all administrative tasks such as configuring the operating mode of Service Now, adding devices discovered by Junos Space Network Management Platform, installing AI-Scripts on devices, configuring SNMP destinations for sending notifications, establishing connection with Juniper Support Systems, and so on. Only a user with Service Now Admin privileges can perform the tasks in the Administration workspace.

Administrative tasks that you can perform depend on the mode in which you configure Service Now to operate. See "Service Now Modes" on page 36 for details.

The Administrative workspace dashboard graphically displays the number of devices in a device group and devices that are not sending snapshots.

You can perform the following tasks from the Administration workspace:

The Administration workspace enables you to perform the following tasks:

- Configure and manage organizations; see "Service Now Organizations Overview" on page 119 for information about organization.
- Configure and manage device groups; see "Service Now Device Groups Overview" on page 137 for information about device groups.
- Add devices discovered by Junos Space Platform and manage the devices; see "Service Now Devices Overview" on page 147 for information about Service Now devices.
- Add AI-Scripts package to Service Now, configure event profiles using the AI-Scripts package and install event profiles on devices; see "AI-Scripts Overview" on page 21 for information about AI-Scripts package and event profiles.
- Configure global settings for Service Now; see "Service Now Global Settings Overview" on page 69 for information about global settings.
- Configure and manage incident filters; see "Service Now Incident Filters Overview" on page 255 for information about incident filters.
- Configure and auto submit filters; see "Service Now Auto Submit Filters Overview" on page 275 for information about auto submit filters.
- Configure and manage auto submit policies; see "Service Now Auto Submit Policy Overview" on page 237 for information about auto submit policies.
- Configure and manage product health data collection on devices; see *Service Now Product Health Data Collection Overview* for information about product health data collection.

- Configure address groups; see “Service Now Address Group Overview” on page 333 for information about address groups.
- Manage e-mail templates; see “Service Now E-Mail Templates Overview” on page 345 for information about e-mail templates.

RELATED DOCUMENTATION

Junos Space Service Now Overview

Service Insight Overview

Service Now Modes

IN THIS SECTION

- Service Now Modes Overview | 37

Service Now Modes Overview

Depending on your contract with Juniper Networks, Junos Space Service Now operates in Direct, End Customer, and Partner Proxy modes. Service Now enables and disables certain features based on its mode of operation.

> **NOTE:** Service Now and Service Insight should be run in the same server group of a JBoss EAP domain as the Junos Space Network Management Platform. Operating Service Now, Service Insight, and Junos Space Network Management Platform in different server groups is not supported.
>
> For information on running Junos Space applications in server groups, refer to *Junos Space Network Management Platform User Guide*.

- Demo mode–Service Now operates in demo mode from the time you install Junos Space and until you create a Service Now organization and validate the organization's connection with JSS.

  In this 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 Systems(JSS). You can perform all Service Now tasks except submit cases, create auto submit policies, view exposure, or view cases in Case Manager. You can use offline mode when you do not want your devices to be connected to the Web such as in military or banking applications.

  You do not have the option to work in offline mode if Service Now is already in the end customer mode.

- Direct mode–In Direct 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 or informational Juniper Message Bundles (iJMBs) ithat you submit.

- End Customer mode–Service Now can be operated in the End Customer mode by small enterprises with few network devices. In this mode, Service Now cannot directly communicate with JSS. Instead Service Now communicates with a Service Now partner who helps the end-customer create technical support cases with JSS.

  Also, the Service Now partner provides credentials to the end customer to create an organization. The customer creates an organization using the credentials, and submits incidents and iJMBs to the partner. The partner submits the cases to JSS and sends case updates back to the customer. JSS validates a customer only when an iJMB or incident is submitted to it.

Direct mode and End Customer mode have similar functions; however, in the End Customer mode, you can create only one organization and you communicate with the Service Now partner instead of JSS.

- Partner Proxy mode–Service Now can be operated in the Partner Proxy mode by a qualified Juniper Networks partner. A Juniper Networks partner manages Service Now applications of multiple end customers. End customers are also known as connected members. A Service Now partner establishes a secure HTTPS connection with all end customers that it manages and with JSS. The Service Now partner receives JMBs from end-customers and either submits the JMBs to JSS on behalf of the end-customers or handles the cases without JSS support.

  In this mode, a partner can add multiple organizations and device groups and associate every customer with an organization. In JSS, each organization is associated with a Site ID and cases from customers are opened with Juniper Networks under the site ID associated with tend-customer's organization.

  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 Service Now partner and the end-customer is encrypted.

Table 4 on page 38 highlights some of the differences in the various modes of operating Service Now.

Table 4: Tasks Enabled for Service Now Modes

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

Table 4: Tasks Enabled for Service Now Modes *(continued)*

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

Table 5 on page 40 lists the differences in the Service Now GUI when Service Now operates in different operating modes.

Table 5: Differences in the Service Now GUI for Different Operating Modes

	Direct Mode	End Customer Mode	Partner Proxy Mode	Offline Mode	Demo Mode
Service Now Notice on dashboard See *Service Now Dashboard Overview*	Service Now is enabled.	Service Now is connected to a Service Now Proxy.	Service Now is enabled as a Partner Proxy	Service Now offline mode is enabled	Service Now is in Demo Mode
Service Insight For information about Service Insight, see Junos Space Service Insight User Guide	Supported	NA	Supported	NA	NA

Table 5: Differences in the Service Now GUI for Different Operating Modes *(continued)*

	Direct Mode	End Customer Mode	Partner Proxy Mode	Offline Mode	Demo Mode
Global settings page For information about configuring global settings, see "Configuring Global Settings" on page 75	Options available for configuring: • Outbound e-mail address Device snapshot purge time Product health Data purge time Submitted incident purge time Not submitted incident purge time Device log file purge time Do not auto submit which are older Repeat incident dampening period Share Service Now Profile Information Collect Log Files **Connection status** refers to connection of Service Now with JSS.	Options available for configuring: • Outbound e-mail address • Device snapshot purge time • Product health Data purge time • Submitted incident purge time • Not submitted incident purge time • Device log file purge time • Do not auto submit which are older • Repeat incident dampening period • Share Service Now Profile Information Collect Log Files **Connection status** refers to connection of Service Now with JSS.	Options available for configuring: • Outbound e-mail address Device snapshot purge time Product health Data purge time Submitted incident purge time Not submitted incident purge time Device log file purge time Do not auto submit which are older Repeat incident dampening period Share Service Now Profile Information Collect Log Files **Connection status** refers to connection of Service Now with JSS.		

Table 5: Differences in the Service Now GUI for Different Operating Modes *(continued)*

	Direct Mode	End Customer Mode	Partner Proxy Mode	Offline Mode	Demo Mode
				Options available for configuring: • Outbound e-mail address Device snapshot purge time Product health Data purge time Submitted incident purge time Not submitted incident purge time Device log file purge time Do not auto submit which are older Repeat incident dampening period Share Service Now Profile Information Collect Log Files **Connection Status** is not	Options available for configuring: • Outbound e-mail address Device snapshot purge time Product health Data purge time Submitted incident purge time Not submitted incident purge time Device log file purge time Do not auto submit which are older Repeat incident dampening period Share Service Now Profile Information Collect Log Files **Connection status** refers

Table 5: Differences in the Service Now GUI for Different Operating Modes *(continued)*

	Direct Mode	End Customer Mode	Partner Proxy Mode	Offline Mode	Demo Mode
				displayed	to connection of Service Now with JSS and is always **Connection Failed**.
Core file configuration For information about configuring FTP server to upload core file, see "Configuring Server to Upload Core Files" on page 84	Contains options to configure FTP and SFTP servers for uploading core file	Displays the FTP server configured for uploading core file. End customers use the FTP server configured by the Service Now partner to upload core files. Therefore end customers do not have the option to configure FTP server	Contains options to configure FTP and SFTP servers for uploading core file	Contains options to configure FTP and SFTP servers for uploading core file	Contains options to configure FTP and SFTP servers for uploading core file
Partner Certificate Configuration For information about configuring partner certificate in an end customer Service Now, see "Service Now End Customer–Partner Communication Overview" on page 107	NA	Can configure the SSL certificate from Service Now partner for secure communication	NA	NA	NA

Table 5: Differences in the Service Now GUI for Different Operating Modes *(continued)*

	Direct Mode	End Customer Mode	Partner Proxy Mode	Offline Mode	Demo Mode
Add member For information about adding end customers to Service Now, see "Adding an End Customer to Service Now Configured in Partner Proxy Mode" on page 125.	NA	NA	Add member option is provided to add end customers to Service Now.	NA	NA
E-mail templates listed For information about E-mail templates, see "Service Now E-Mail Templates Overview" on page 345.	E-mail templates for flagging and submitting incidents; creating and updating case; flagging messages to users; new incidents are created; iJMBs are received, expiry of certificates; failure to collect product health data; activities related to end customer cases	E-mail templates for flagging and submitting incidents; creating and updating case; flagging messages to users; new incident creation; iJMBs are received, iJMBs are not received, expiry of certificates; failure to collect product health data	E-mail templates for flagging and submitting incidents; creating and updating case; flagging messages to users; new incident creation; iJMBs are received, iJMBs are not received; failure to collect product health data	E-mail templates for flagging new incidents, iJMBs received, failute to collect product health data	No e-mail templates are listed
End customer cases For information about end customer cases, see *Service Now Technical Support Cases and End Customer Support Cases Overview*.	NA	NA	Includes the option View End Customer Cases to view cases submitted by end customers for resolution	NA	NA

Table 5: Differences in the Service Now GUI for Different Operating Modes *(continued)*

	Direct Mode	End Customer Mode	Partner Proxy Mode	Offline Mode	Demo Mode
Submitting Incidents For information about submitting incidents, see *Submitting an Incident to Juniper Support Systems or Service Now Partner*.	Site ID and username can be modified	Site ID not visible for end customers	Site ID and username can be modified	NA	NA
Generating on-demand Incidents For information about creating on-demand incidents, see "Generating an On-Demand Incident" on page 174.	The Creating On-demand Incidents page contains the following options: • Automatically Submit incident -Use Service Now to generate Incident -Collect log files -Verify CPU Usage	The Creating On-demand Incidents page contains the following options: • Automatically Submit incident -Use Service Now to generate Incident	The Creating On-demand Incidents page contains the following options: • Automatically Submit incident -Use Service Now to generate Incident -Collect log files -Verify CPU Usage	The Creating On-demand Incidents page contains the following options: • Automatically Submit incident -Use Service Now to generate Incident -Collect log files -Verify CPU Usage	The Creating On-demand Incidents page contains the following options: • Automatically Submit incident -Use Service Now to generate Incident -Collect log files -Verify CPU Usage

RELATED DOCUMENTATION

Configuring Global Settings | **75**

Adding an Organization to Service Now | **122**

Adding an End Customer to Service Now Configured in Partner Proxy Mode | **125**

Discovering Devices

Devices are discovered by Junos Space Network Management Platform. You can use Service Now to select the discovered devices on which you want to monitor faults. For information about discovering devices see Discovering Devices by Using Junos Space Network Platform.

RELATED DOCUMENTATION

- Service Now Device Groups Overview | 137
- Creating a Device Group | 138
- Adding Devices to Junos Space Service Now | 155

Juniper Networks Devices Supported by Service Now and Service Insight

Table 6 on page 47 lists all the Juniper Networks product series and devices supported by Junos Space Service Now Release 18.1R1 and AI-Scripts Release 7.0R4. For information about devices supported by Junos Space Network Management Platform, see Devices Supported by Junos Space Network Management Platform.

Table 6: Devices Supported by Junos Space Service Now

Product Series	Devices
ACX Series	ACX500 ACX1000 ACX1100 ACX2000 ACX2100 ACX2200 ACX4000 ACX5000 ACX5048 ACX5096

Table 6: Devices Supported by Junos Space Service Now *(continued)*

Product Series	Devices
EX Series	EX2200
	EX2300
	EX3200
	EX3300
	EX3400
	EX4200
	EX4200-Copper
	EX4300
	EX4500
	EX4550
	EX4550-40G
	EX4600
	EX6200
	EX6210
	EX8208
	EX8216
	EX9200
	EX9204
	EX9208
	EX9214
	Junos Fusion Data Center
	Junos Fusion Enterprise

Table 6: Devices Supported by Junos Space Service Now *(continued)*

Product Series	Devices
EX Virtual Chassis	EX3300-VC EX4200-VC EX4300-VC EX4500-VC EX4550-VC EX9204-VC EX9208-VC MIXED-MODE-EX-VC EX-XRE
FireFly	vSRX Firefly
J Series	J2320 J2350 J4350 J6350
Junos Fusion	Junos Fusion Data Center Junos Fusion Edge Junos Fusion Enterprise
LN Series	LN1000 LN2600
M Series	M7i M10i M40e M120 M320

Table 6: Devices Supported by Junos Space Service Now *(continued)*

Product Series	Devices
MX Series	MX5 MX10 MX80 MX104 MX240 MX480 MX960 MX2008 MX2010 MX2020 MX10003 MX10008 MX10016 Junos Fusion Data Center
MX Series Virtual Chassis	MX-VC
PTX Series	PTX1000 PTX3000 PTX5000 PTX10008 PTX10016

Table 6: Devices Supported by Junos Space Service Now *(continued)*

Product Series	Devices
QFX Series	QFX3000 QFX3000-G QFX3000-M QFX3500 QFX3600 QFX5100 QFX5100-96S QFX5110-32Q QFX5110-48S QFX5100-96S QFX5200 QFX10002 QFX10002-36Q QFX10002-36Q-DC QFX10002-72Q QFX10002-72Q-DC QFX10008 QFX10016 **NOTE:** QFX3000, QFX3000-G, and QFX3000-M are supported only in AI-Scripts 4.1 as part of QFabric.
QFX Series Virtual Chassis	QFX-VC

Table 6: Devices Supported by Junos Space Service Now *(continued)*

Product Series	Devices
SRX Series	SRX100 SRX110H-VB SRX210 SRX220 SRX240 SRX300 SRX320 SRX320-PoE SRX340 SRX345 SRX550 SRX550-M SRX650 SRX1400 SRX1500 SRX3400 SRX3600 SRX4100 SRX4200 SRX5400, SRX5600, SRX5800
Virtual SRX Series	Firefly Perimeter, vSRX **NOTE:** vSRX devices running Junos OS release earlier than Junos OS 15.1x are called Firefly Perimeter.

Table 6: Devices Supported by Junos Space Service Now *(continued)*

Product Series	Devices
T Series	T320 T640 T1600 T4000 TX Matrix TX Matrix Plus TXP-3D
Virtual MX Series	vMX
Virtual route reflector (VRR)	VRR

RELATED DOCUMENTATION

Adding Devices to Junos Space Service Now | 155

Installing AI-Scripts on a Device

Service Now Domain Overview

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

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

When you log in to Service Now, objects in the system domain and objects such as organization, script bundle, SNMP configuration, and Email template, which are assigned to the domain that you are currently in, are visible to you. If you are assigned to more than one domain, you can access the other domains and

objects in those domains by selecting the domains from the **Login as *username* in** list present on the Service Now banner. Only the domains to which you are assigned are listed. A super user can access all domains.

Objects that you create when you are logged in to a certain domain are assigned to that domain. However, if you have administrative privileges, you can assign the objects to another domain. For information about changing the domain of an object, refer to "Assigning a Service Now Object to Another Domain" on page 56.

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

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

When the device is assigned to a domain, objects such as technical or end-customer support cases that are not assigned to any device belong to the domain assigned to the organization associated with the device. Table 7 on page 54 lists Service Now objects and their default domains.

Table 7: Service Now Objects and Their Default Domains

Service Now Objects	Default Domain	
	Fresh Installation	Migration
• Organization • Connected Member • Device Group • Address Group • Notification • Auto Submit Policy • Event Profile • Product Health Data Configuration • Auto Submit Filter • Incident Filter	Domain to which a user is logged in	Global domain

Table 7: Service Now Objects and Their Default Domains *(continued)*

Service Now Objects	Default Domain	
	Fresh Installation	Migration
• Global Setting • Directive File • SNMP Configuration • Core File Upload Configuration • Message • Script Bundle • Email Template • End Customer Information Message • Script Installation Advisor (SIA)	System domain	System domain
• Service Now Device • Incident • Device Snapshot • Error JMB • Technical Support Case • End Customer Case	Domain assigned to the device in Junos Space Network Management Platform	Domain assigned to the device in Junos Space Network Management Platform

Assigning a Service Now Object to Another Domain

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

To assign a Service Now object to another domain:

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

   The object's page appears.

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

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

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

   The Assign to Domain dialog box appears.

4. Under Assign selected items to domain, select the domain to which you want to assign the object and click **Assign**.

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

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

   The Service Now GUI is refreshed.

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

RELATED DOCUMENTATION

Service Central Overview

Service Now Administration Workspace Overview | 35

Domains Overview

3

CHAPTER

Installing, Upgrading, and Uninstalling Junos Space Service Now

Installing Junos Space Service Now and Junos Space Service Insight Applications | 59

Upgrading Junos Space Service Now and Junos Space Service Insight Applications | 63

Uninstalling Junos Space Service Now and Junos Space Service Insight Applications | 65

Installing Junos Space Service Now and Junos Space Service Insight Applications

IN THIS SECTION

- Uploading a Service Now and Service Insight Image File to a Junos Space Server | 59
- Installing Junos Space Service Now and Junos Space Service Insight | 61

Junos Space Service Now Release 18.1R1 and Junos Space Service Insight Release 18.1R1 are supported only on Junos Space Network Management Platform Release 18.4R1. You must upgrade earlier releases of Service Now and Service Insight to 18.1R1 release for operating Service Now and Service Insight Release 18.1R1 on Junos Space Platform Release 18.4R1.

CAUTION: If Service Now and Service Insight are already installed on a Junos Space server, do not uninstall them to install or upgrade to a later version. Uninstalling deletes all the Service Now and Service Insight data from the Junos Space server. To upgrade Service Now and Service Insight to a later version, use the upgrade option in the Junos Space Network Management Platform. For details, see "Upgrading Junos Space Service Now and Junos Space Service Insight Applications" on page 63.

This topic discusses the following:

Uploading a Service Now and Service Insight Image File to a Junos Space Server

Before you upgrade or install Service Now and Service Insight, you must upload the required Service Now image file to a Junos Space server.

NOTE:

- Service Insight is combined with Service Now in the Service Now image file. You can access Service Insight based on your license for support contract.
- You cannot access Service Insight if you are operating Service Now in the End Customer mode.

To upload a Service Now image file to a Junos Space server:

1. Download the Service Now image file from the Juniper Networks support site at https://www.juniper.net/support/downloads/?p=servicenow#sw to your local file system.

2. Log in to the Junos Space Platform with the default username and password (**super/juniper123**).

3. From the Junos Space Network Management Platform navigation tree, select **Administration** > **Applications**.

   The Applications page appears.

4. On the top-left corner of the Applications page, click the **Add Applications** icon:

   .

   The Add Application page appears.

5. On the Add Application page, perform one of the following tasks:

   - Upload the Service Now image file by using HTTP.
     a. Click **Upload via HTTP**.

        The Upload Software via HTTP dialog box appears.

     b. Type the name of the Service Now image file or click **Browse** to navigate and select the Service Now image file on the local file system.

     c. Click **Upload**.

     NOTE: Upload the Service Now image file by using SCP if you receive the following message:

     File size is too big, use scp to upload this file.

   - Upload the Service Now image file by using SCP.
     a. Click the **Upload via SCP** button.

The Upload Software via SCP dialog box appears.

b. Enter the following details for the image file to be uploaded by using SCP:

- Username: Enter your username for the local file system.
- Password: Enter your password for the local file system.
- Confirm Password: Retype your password.
- Machine IP: Enter the host IP address of the local file system.
- Software File Path: Specify the file path to access the Service Now image file on the local file system.

c. Click **Upload**.

The process of uploading the Service Now image file to the Junos Space server begins and the Upload Application Job Information dialog box appears.

6. In the Upload Application Job Information dialog box, click the *Job ID* link.

   The Job Management page is displayed. This page displays the progress of the upload job.

7. After the upload job is complete, go to **Administration** > **Applications** on the navigation tree to verify the upload.

   The Applications page appears.

8. Click the **Add Application** icon.

   The Add Application page appears. The uploaded Service Now image file should be listed on this page.

Installing Junos Space Service Now and Junos Space Service Insight

Before you install:

- You must ensure that the version of Service Now and Service Insight that you want to install are compatible with the Junos Space Network Management Platform version installed on the Junos Space Server. For information on Junos Space Network Management compatibility, refer to Junos Space Application Compatibility Matrix.

  If the installed Junos Space Platform version is earlier than the compatible version, upgrade the Junos Space Platform to the compatible release first and then upgrade Service Now and Service Insight applications. For information about upgrading Junos Space Network Management Platform, see *Upgrading Junos Space Network Management Platform Overview*.

- Upload the Service Now image file to Junos Space server. See "Uploading a Service Now and Service Insight Image File to a Junos Space Server" on page 59 for information about uploading an image file to the Junos Space server.

To install Service Now and Service Insight applications:

1. Log in to Junos Space Network Management Platform using the default Username and password (super/juniper123).

2. In the navigation tree, click **Administration** > **Applications**.

   The Applications page appears.

3. On the top-left corner of the Applications page, click the Add Applications icon: .

   The Add Application page appears.

4. In the Add Application page, do one of the following:

   - If the Service Now Release that you want is listed, select it and click **Install**.

     The Application Configuration window appears indicating that no configuration input is required..

   - If the Service Now Release that you want is not listed, you must upload the release to Junos Space server.

     To upload a Service Now image file to Junos Space server, see "Uploading a Service Now and Service Insight Image File to a Junos Space Server" on page 59.

5. Click OK.

   A job is created for the installation process and the Application Management Job Information dialog box appears.

6. In the Application Management Job Information dialog box, click the *Job ID* link. The Job Management page is displayed. This page displays the progress of the upload job.

7. After the installation job is complete, log out of Junos Space GUI and log in again to access Service Now. Service Now should be listed in the drop-down menu present above the Junos Space Network Management Platform navigation tree.

RELATED DOCUMENTATION

Service Now Global Settings Overview | 69

Configuring Global Settings | 75

Upgrading Junos Space Service Now and Junos Space Service Insight Applications

From Junos Space Network Management Platform Release 14.1 onwards, Junos Space Service Now and Junos Space Service Insight are available as hot-pluggable applications. This allows you to upgrade and uninstall Service Now and Service Insight applications independent of the Junos Space Network Management Platform.

Service Insight is bundled with the Service Now image file and is upgraded along with Service Now.

> **CAUTION:** Do not uninstall the installed versions of Service Now and Service Insight for upgrading to a later version. Uninstalling the applications deletes all Service Now and Service Insight data from the Junos Space server.

You can upgrade to Service Now Release 18.1R1 and Service Insight Release 18.1R1 from the Service Now Release 17.2R1 and Service Insight Release 17.2R1.

Before you upgrade Junos Space Service Now and Junos Space Service Insight:

- Ensure that versions of Service Now and Service Insight to which you want to upgrade are compatible with the Junos Space Platform version installed on the Junos Space server. For information about compatibility of the Junos Space Platform with Service Now and Service Insight, refer to Junos Space Application Compatibility Matrix.

  If the installed Junos Space Platform version is earlier than the compatible version, upgrade the Junos Space Platform to a compatible release first and then upgrade the Service Now and Service Insight applications. For information about upgrading the Junos Space Platform, refer to Junos Space Software Upgrade FAQs.

- Upload the Service Now image file to the Junos Space server. See "Uploading a Service Now and Service Insight Image File to a Junos Space Server" on page 59 for information about uploading a Service Now and Service Insight image file to a Junos Space server.

To upgrade Junos Space Service Now and Junos Space Service Insight applications:

1. Log in to the Junos Space Platform with the default username and password (**super/juniper123**).

2. From the Junos Space Network Management Platform navigation tree, select **Administration** > **Applications**.

   The Applications page appears.

3. On the Applications page, click **Service Now** and select **Actions** > **Upgrade Application**. Alternatively, right-click **Service Now** and select **Upgrade Application**.

   The Upgrade Application page appears displaying all the previously uploaded versions of Service Now.

4. On the Upgrade Application page, perform one of the following tasks:

   - If the Service Now release to which you want to upgrade is listed, select the ***Service Now release*** to which you want to upgrade and click **Upgrade**.
   - If the Service Now release to which you want to upgrade is not listed, upload the Service Now image file to the Junos Space server and then click **Upgrade**.

     To upload a Service Now image file to the Junos Space server, see "Uploading a Service Now and Service Insight Image File to a Junos Space Server" on page 59.

     A job is created for the upgrade process and the Application Management Job Information dialog box appears.

5. In the Application Management Job Information dialog box, click the ***Job ID*** link. The Job Management page is displayed. This page displays the progress of the upload job.

6. After the upgrade job is complete, navigate to **Administration** > **Applications**.

   The Applications page lists the upgraded releases of Service Now and Service Insight installed on Junos Space server.

RELATED DOCUMENTATION

Installing Junos Space Service Now and Junos Space Service Insight Applications | **59**

Uninstalling Junos Space Service Now and Junos Space Service Insight Applications | **65**

Service Now Global Settings Overview | **69**

Configuring Global Settings | **75**

Adding an SNMP Configuration to Service Now | **80**

Uninstalling Junos Space Service Now and Junos Space Service Insight Applications

From Junos Space Network Management Platform Release 14.1 onwards, Junos Space Service Now and Junos Space Service Insight are available as hot-pluggable applications. This allows you to uninstall Service Now and Service Insight applications independent of the Junos Space Network Management Platform.

To uninstall Service Now and Service Insight applications:

1. Log in to the Junos Space Platform with the default username and password (**super/juniper123**).

2. From the navigation tree, select **Administration** > **Applications**.

   The Applications page appears.

3. On the Applications page, click **Service Now** and select **Actions** > **Uninstall Application**. Alternatively, right-click Service Now and select **Uninstall Application**.

   The progress of the uninstallation process is displayed. After the uninstallation is complete, Service Now and Service Insight applications are not listed on the Applications page.

RELATED DOCUMENTATION

Upgrading Junos Space Service Now and Junos Space Service Insight Applications | 63

Uninstalling Junos Space Service Now and Junos Space Service Insight Applications | 65

4

CHAPTER

Managing Global Settings

Service Now Global Settings Overview | **69**

Configuring Global Settings | **75**

Adding an SNMP Configuration to Service Now | **80**

Editing an SNMP Configuration | **81**

Managing SNMP Traps | **82**

Viewing Proxy Server Settings Configured on the Junos Space Platform | **84**

Configuring SFTP Server for Uploading Core Files Generated for Events | **84**

Directive File Overview | **86**

Updating the Directive File in Junos Space Service Now | **88**

Restoring the Default Directive File | **91**

Configuring Advanced Filter Settings | **92**

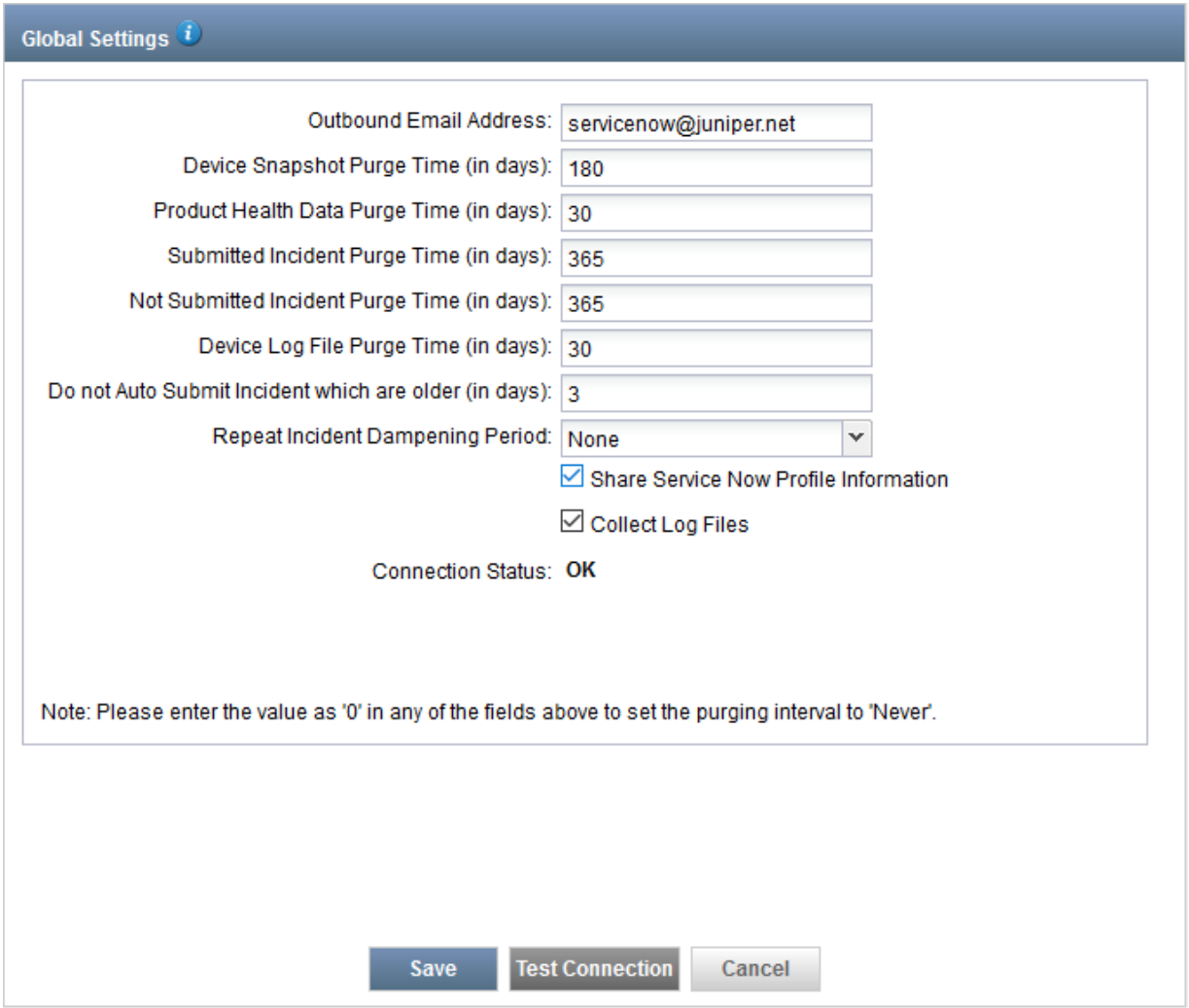
Service Now Global Settings Overview

The Junos Space Service Now Global Settings task lets you configure the general behavior of Junos Space Service Now. After you install Service Now and configure it to operate in a specific mode, you must configure parameters on the Global Settings page (**Administration > Global Settings**).

NOTE: You must have Service Now administrator privileges to configure global settings.

Figure 3 on page 69 shows the Global Settings page.

Figure 3: Global Settings Page



The Global Settings task also provides options to a Service Now end customer to import and install SSL certificates from a Service Now partner to establish secured connection with the Service Now partner. For information about installing an SSL certificate of a Service Now partner, see "Installing the SSL Certificate on a Service Now End Customer" on page 113.

After a connection is established between a Service Now application operating in End Customer mode with the Service Now partner, you can add an organization using the credentials provided by the Service Now partner. For information about adding an organization, see "Adding an Organization to Service Now" on page 122. After the connection of the organization is validated, you can submit incidents and iJMBs to the Service Now partner.

If you select the **Share Service Now Profile Information** option on the Global Settings page, you can periodically send data related to incident activities, devices, event policies, and Junos Space operations to JSS or a Service Now partner. Service Now uploads the data in an XML file and sends the XML file to JSS by using **MetadataUploadRequest**. These files are uploaded to JSS once a week.

Information about the following elements is collected in the XML file.

- Fabric nodes
- Application summaries
- Devices
- Organization
- Event profiles
- Incidents

Table 8: XML File Information

SpaceInfo—Specifies information about Junos Space

Table 8: XML File Information *(continued)*

FabricInfo—Specifies information about a node in Junos Space fabric

- RowID: ID of the element
- Name of the fabric node: Name of the fabric node
- Status: Status of the fabric node
- CPU: Percentage of CPU used by the fabric node
- RAM: Percentage of RAM used by the fabric node
- Disk: Percentage of disk used by the fabric node
- AppLogic: Specifies whether the application logic function is up or down on the node
- Database: Specifies whether the database function is up or down on the node
- LoadBalancer: Specifies whether the load balancing function is up or down on the node
- HardwareModel: Hardware model of the fabric node
- SoftwareVersion: Version of software installed on the fabric node
- IsMasterNode: This value is set to true only if the fabric node is the primary node
- IsVIPNode: This value is set to true only if the fabric node is a VIP node

ApplicationSummary—Specifies information about the applications installed on Junos Space

- Application: Container tag for application information
- RowID: ID of the element
- AppName: Name of the application
- AppVersion: Version of the application
- ReleaseType: Release type of the application
- Build: Build number of the application
- IsEnabled: This value is set to true only if the application is enabled in Junos Space.
- Date: Date and time of collecting application summary information

Table 8: XML File Information *(continued)*

DevicesInfo—Specifies Information about the devices managed by Junos Space Network Management Platform

- Device: Container tag for device information
- RowID: ID of the element
- OSVersion: Version of Junos OS installed on the device
- Product: Product type of the device
- SchemaVersion: Version of the Junos OS schema
- ConnectionStatus: Status of the connection between Junos Space and the device
- PrimarySiteID: Default site ID of the organization to which the device belongs
- SiteID: Site ID of the organization to which the device belongs
- AIScriptVersion: Version of AI-Scripts installed on the device
- IsMangedBySN: Specifies whether the device is managed by Service Now; true indicates that the device is managed by Service Now.
- ProfileName: Name of the event profile installed on the device
- SerialNumber: Serial number of the device
- RoutingEngine: In case of dual Routing Engines, this element specifies the primary Routing Engine.

ApplicationDetails—Specifies detailed information about the application installed on Junos Space. Currently, only Service Now is supported.

- Application name: Name of the application

OrganizationInfo—Specifies information about the organizations in Service Now

- TotalConnectedMembers: Total number of connected members connected to the partner Service Now
- Organization: Container tag for organization information
- RowID: ID of the element
- Name: Name of the organization
- PrimarySiteID: Primary site ID of the organization
- SecondarySiteIDs: List of secondary site IDs of the organization
- UserName: Username of the organization
- ConnectionStatus: Connection status of the organization
- JMBFilterLevel: Filter level of the JMB
- Status: Case submission status
- IsConnectedMember: This value is set to true only if it is a connected member.

Table 8: XML File Information *(continued)*

EventProfilesInfo—Specifies information about the event profiles installed on the devices

- EventProfile: Container tag for the event profile information
- RowID: ID of the element
- Name: Name of the event profile that is installed
- EventsIncluded: Total number of events included in the event profile
- EventsExcluded: Total number of events excluded from the event profile
- AIScriptVersion: Version of the AI-Scripts bundle from where the profile is created
- TotalEventsInBundle: Total number of events in the AI-Scripts bundle
- EventsWithNoIncidents: Total number of events in the profile for which no incidents are reported to Service Now
- TotalIncidents: Total number of incidents in Service Now for this profile
- AssociatedDevicesCount: Total number of devices on which this event profile is installed
- EventsInfo: List of events present in this event profile

IncidentsInfo—Information about incidents in Service Now that are in the initial state

- Incident: Container tag for incident information
- RowID: ID of the element
- ID: Incident ID. This is a CDATA section.
- Synopsis: Incident synopsis. This is a CDATA section.
- ProblemDescription: Problem description of this incident
- Organization: Name of the organization with which this device is associated in Service Now
- PrimarySiteID: Primary site ID of the organization to which this device belongs
- SiteID: Site ID of the organization to which this device belongs
- Priority: Priority of the incident
- Severity: Severity of the incident
- Type: Type of the incident
- DefectType: Type of defect that caused this incident
- EventType: Event type that caused this incident
- DeviceSerialNumber: Serial number of the device on which this incident occurred
- Release: Junos OS release installed on the device
- Version: Junos OS release version installed on the device
- Product: Product type of the device
- Platform: Platform type of the device

Global Settings allows you to configure the following parameters to define the behavior of Service Now:

- E-mail address to be used for e-mails sent by Service Now
- Purge time for device snapshots, incidents that are submitted, incidents that are not submitted, product health data, and device log files
- Time period during which no incident must be created in Service Now when an event reoccurs on a device
- Time period after which incidents generated should not be submitted by using auto submit policies
- Configure whether you want to share Service Now profile information
- Configure whether you want to collect log files from all the managed devices
- Test and verify connection of Service Now with Juniper Support Systems (JSS) when Service Now is operating in Partner Proxy or Direct mode or test connection with the Service Now partner when Service Now is operating in End Customer mode

Associated Actionsk

Apart from configuring parameters, you can perform the following actions to define the behavior of Service Now:

- Configure server for uploading core files; see "Configuring SFTP Server for Uploading Core Files Generated for Events" on page 84 for details.
- Manage directive file; see "Directive File Overview" on page 86 for details.
- Configure advanced settings; see "Configuring Advanced Filter Settings" on page 92 for details.

RELATED DOCUMENTATION

Configuring Global Settings | **75**

Service Now Modes | **36**

Service Now Device Snapshots Overview

Product Health Data Collection Configuration Overview | **297**

Configuring Global Settings

After installing Junos Space Service Now and configuring it to operate in a specific mode, you must configure the global settings to define purge time for device snapshots, incidents, log files, and BIOS attachments.

Starting in Service Now Release 16.1R1, the **Submitted Incident Purge Time (in days)** and **Not Submitted Incident Purge Time (in days)** fields are available on the Global Settings page to define the number of days after which incidents that are submitted to JSS and incidents that are not submitted to JSS can be purged respectively

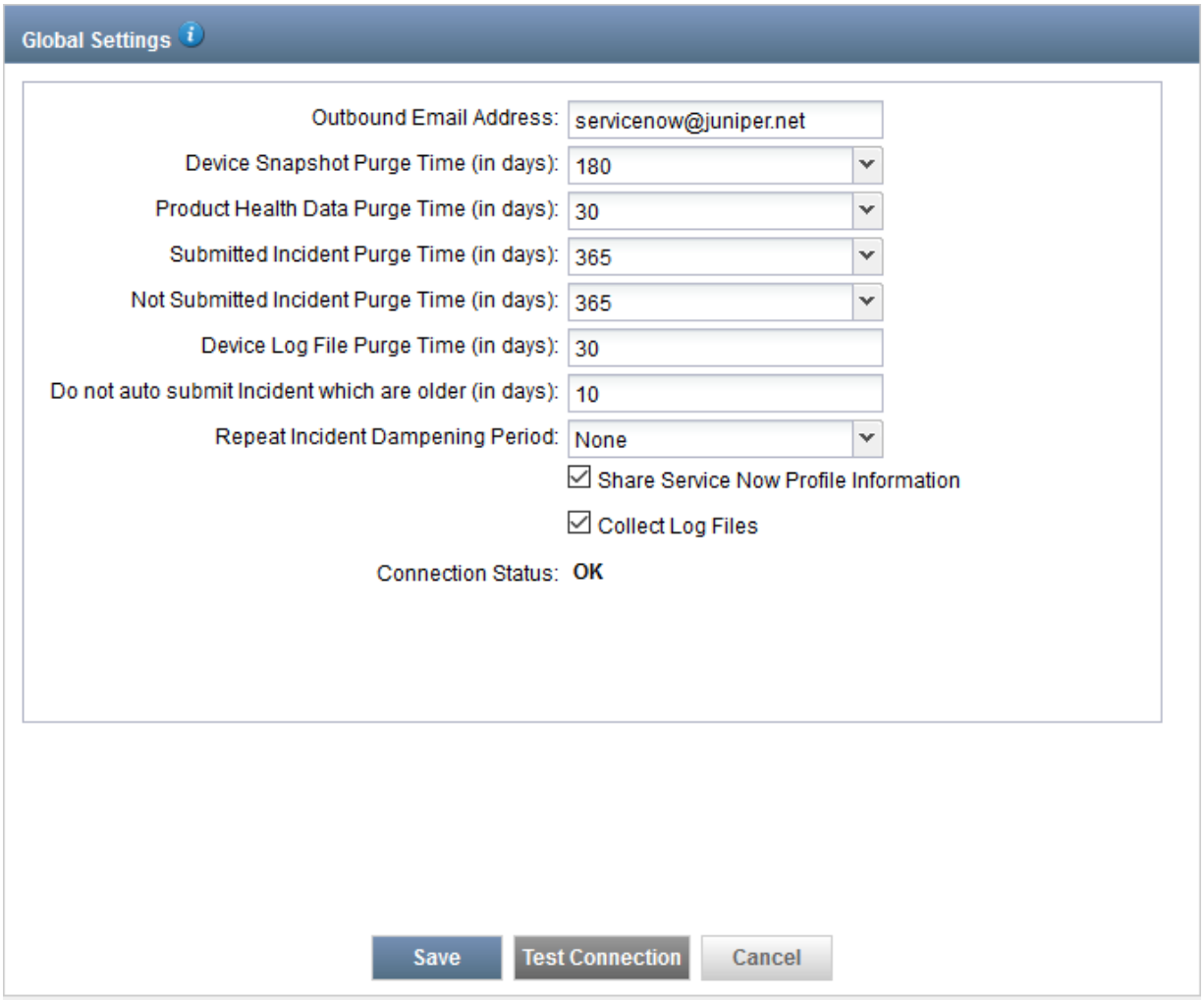
Starting in Service Now Release 16.1R1, the **Do not auto submit Incident which are older (in days)** is available on the Global Settings page to prevent incidents older than the number of days specified in the field from being submitted to JSS by auto submit policies.

To configure Service Now global settings:

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

   The Global Settings page appear as shown in Figure 4 on page 76.

Figure 4: Global Settings Page



2. Enter values for the global settings as described in Table 9 on page 77.

3. Click **Save** to save the global settings and update Service Now or click **Cancel** to navigate back to the Global Settings page without saving the entries.

   If you click the information icon displayed next to the Global Settings page heading, the Help page for configuring global settings is displayed.

Table 9 on page 77 describes the fields displayed on the Global Settings page.

Table 9: Global Settings Parameters

Name	Description	Range/Length	Default
Outbound Email Address	E-mail address that the recipients of e-mails from Service Now see (for example, exampleservicenow@juniper.net)		
Device Snapshot Purge Time (in days)	Number of days device snapshots of a device are stored in the Service Now database before they are deleted 0 indicates that device snapshots are never purged.	• 0 • 90 • 120 • 180 • 365	180
Product Health Data Purge Time (in days)	The number of days the information about product health data (PHD) is stored in Service Now database. **0** indicates that the information about PHD is never deleted from the database.	• 0 • 30 • 45 • 60 • 90 • 120 • 180 • 365	30
Submitted Incident Purge Time (in days):	Number of days incidents submitted to JSS are stored in the Service Now database before they are deleted 0 indicates incidents submitted to JSS or Service Now partner are never purged.	• 0 • 30 • 45 • 60 • 90 • 120 • 180 • 365	365
Not Submitted Incident Purge Time (in days):	Number of days incidents that are not submitted to JSS are stored in the Service Now database before they are deleted 0 indicates incidents that are not submitted to JSS or Service Now partner are never purged.	• 0 • 30 • 45 • 60 • 90 • 120 • 180 • 365	365

Table 9: Global Settings Parameters *(continued)*

Name	Description	Range/Length	Default
Device Log File Purge Time (in days)	Number of days log files collected from devices are stored in the Service Now database before they are deleted.	1 – 365	30
Do not Auto Sbbmit Incident which are older (in days):	Number of days after which incidents are not submitted to JSS by using auto submit policies	1 – 365	3
Repeat Incident Dampening Period	The time period during which Service Now does not create new incidents on receipt of JMBs for the same event from a device. In other words, if the same event occurs on a device multiple times during the specified time interval, Service Now creates an incident only for occurrences of the event on the device. This value can be overridden by configuring a dampening period for each event in the Auto Submit Policy. For information about the Auto Submit Policy, see "Creating an Auto Submit Policy" on page 239.	• None—Always creates the incident. • Always—Does not create the incident after the first occurrence of the event on the selected devices. • 1hr – 12hr • 1 day – 5 days • 10 days • 15 days • 20 days • 25 days • 30 days • 45 days • 60 days • 90 days • 120 days	None
Share Service Now Profile Information	If this check box is selected, all Service Now-related information is shared with JSS or Service Now partner for tracking purposes. This option is not available in Offline mode.		Service Now-related information is shared with JSS or Service Now partner.

Table 9: Global Settings Parameters *(continued)*

Name	Description	Range/Length	Default
Collect Log Files	If this check box is selected, log files are collected from all Service Now devices. This behavior is overridden by log collection settings configured on individual Service Now devices.		Logs are collected from Service Now devices.
Connection Status	Status of the connection from Service Now to JSS or Service Now partner.	• OK • No route to host • Connection refused • The Home Base server is temporarily unable to service your request	

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16.1R1, the **Submitted Incident Purge Time (in days)** and **Not Submitted Incident Purge Time (in days)** fields are available on the Global Settings page to define the number of days after which incidents that are submitted to JSS and incidents that are not submitted to JSS can be purged respectively
16.1R1	Starting in Service Now Release 16.1R1, the **Do not auto submit Incident which are older (in days)** is available on the Global Settings page to prevent incidents older than the number of days specified in the field from being submitted to JSS by auto submit policies.

RELATED DOCUMENTATION

Service Now Incidents Overview

Service Now Device Snapshots OverviewService Now Product Health Data Collection Overview

Service Now Product Health Data Collection Overview

Adding an SNMP Configuration to Service Now

Junos Space Service Now provides the SNMP configuration task to specify a destination for SNMP traps to be sent when a Service Now notification policy is triggered. SNMP traps are sent to the specified destination only when the notification policy specifies the SNMP traps to be sent. You can view the SNMP trap destinations on the SNMP Configurations page (**Service Now** > **Administration** > **Global Settings** > **SNMP Configuration**).

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

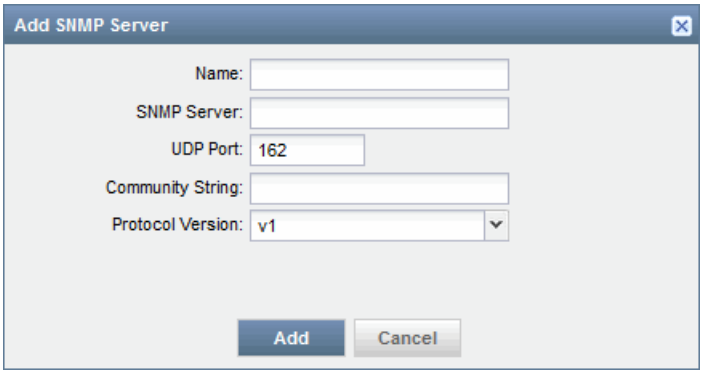
To add an SNMP server:

1. From the Service Now navigation tree, 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.

   The name must begin with an alphanumeric character. Underscore (_), hyphen (-) and space are allowed. The maximum number of characters allowed is 64.

4. In the **SNMP Server** field, enter the IP address or hostname of the network management server where Service Now SNMP traps are sent.

5. In the **UDP Port** text box , enter the UDP port number.
   The default UDP Port number is 162.

6. In the **Community String** text box, 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 SNMP version you want to use from the **Protocol Version** drop-down list.

8. Click **Add**.

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

Loading MIBs

When using a MIB browser or other SNMP trap receivers such as HP OpenView to monitor the devices, the following MIB files must be loaded:

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

> **NOTE:** The **jnx-smi.mib** file must be loaded first.

RELATED DOCUMENTATION

Service Now Notification Policies Overview

SNMP MIBs Downloads

Editing an SNMP Configuration

An SNMP configuration defines the destination for SNMP traps that Service Now sends when a Service Now notification policy is triggered. If you have Service Now Administrator privileges, you can modify the SNMP configuration and also delete them.

Editing an SNMP Configuration

To edit an SNMP configuration:

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

   The SNMP Configuration page appears.

2. Select the SNMP server configuration that 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.

6. (Optional) To verify, you can view the changes on the SNMP Configurations page.

RELATED DOCUMENTATION

SNMP MIBs Downloads

Managing SNMP Traps

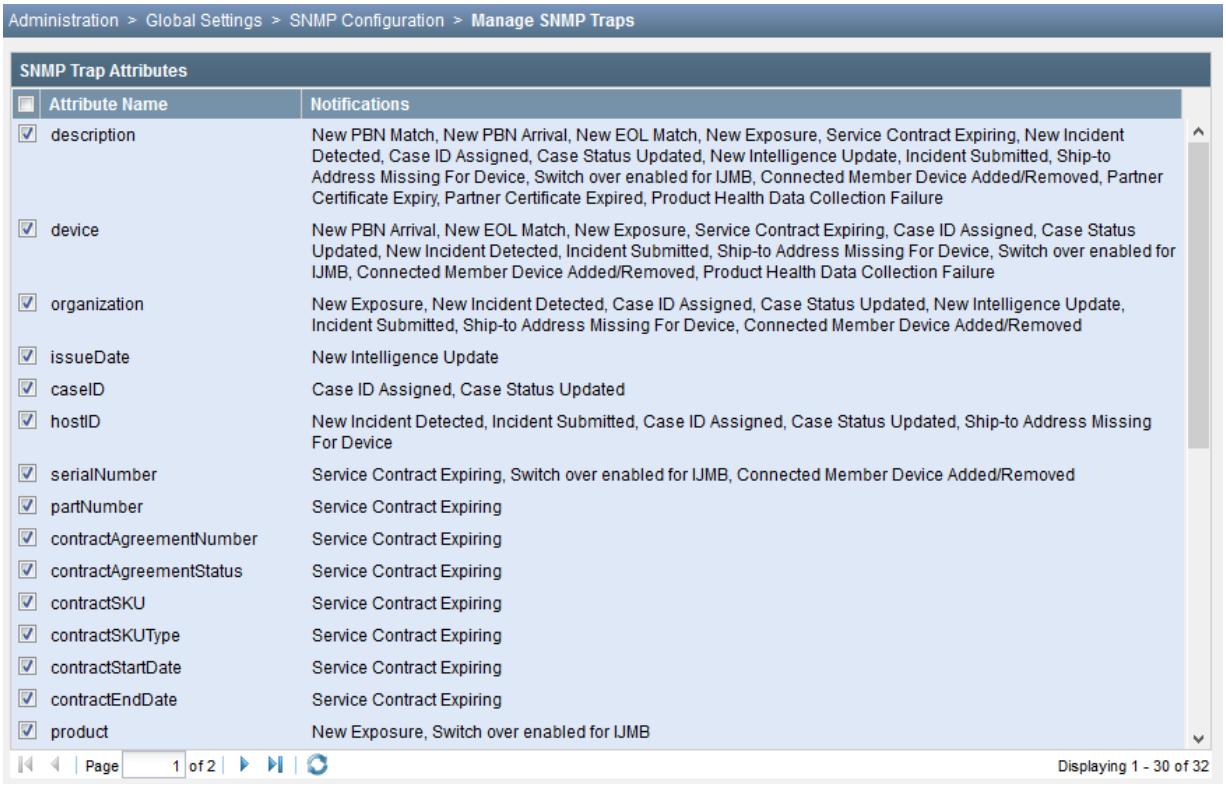
Service Now users can choose to enable or disable an SNMP trap attribute to be added for a notification. To manage SNMP traps, you must have Service Now administration privileges.

To Manage SNMP traps, from the Service Now navigation tree, select **Administration** > **Global Settings** > **SNMP Configuration** > **Manage SNMP Traps**. The SNMP Traps Attributes page appears.

This page displays all the available trap attributes and also the notifications in which these trap attributes are used. See Figure 5 on page 83.

An attribute is added to a notification if the check box next to it is selected. To add or remove attributes from notifications, select or clear the check box for an attribute. By default, all attributes for all notifications are selected.

Figure 5: SNMP Trap Attribute Page



NOTE:

Notifications related to Service Insight are shown on this page only if Service Insight is enabled.

RELATED DOCUMENTATION

- SNMP MIBs Downloads

Viewing Proxy Server Settings Configured on the Junos Space Platform

From Junos Space Service Now Release 14.1 and Junos Space Service Insight Release 14.1, Service Now and Service Insight use the proxy server configured on the Junos Space Network Management Platform to facilitate communication.

> **NOTE:** When upgrading to Service Now Release 14.1, the proxy server configured on Service Now is migrated to the Junos Space Platform if no proxy server is configured on the Junos Space Platform. If a proxy server is already configured on the Junos Space Platform, Service Now uses the proxy server configured on the Junos Space Platform.

To view the proxy server settings that Service Now and Service Insight use, navigate to **Network Management Platform** > **Administration** > **Proxy Servers** on the Junos Space Network Management Platform navigation tree. The Proxy Server page lists the proxy servers configured on Network Management Platform.

RELATED DOCUMENTATION

Configuring Proxy Server Settings in Network Management Platform

Configuring Global Settings | **75**

Adding an SNMP Configuration to Service Now | **80**

Configuring SFTP Server for Uploading Core Files Generated for Events

> **NOTE:** From starting of the year 2018, Juniper Networks does not support uploading core files to an FTP server; you can only upload core files to an SFTP server.

You can configure an SFTP server in Service Now to upload core files that are generated for an event or related to an event. A core file is generated when a fault occurs on a device. You can upload specific core

files either when an incident is submitted to Juniper Support Systems (JSS) or Service Now partner to open a case for the event or after the case is opened.

You can configure an SFTP server only if Service Now is operating in the Partner Proxy, Direct, or Demo mode. In the End Customer mode, Service Now uses SFTP server configured by the Service Now partner to upload core files. The core files are uploaded to the SFTP server and associated with the case number assigned to the incident by the partner. The Service Now partner uploads the core files to JSS where it is associated with the case number provided by JSS.

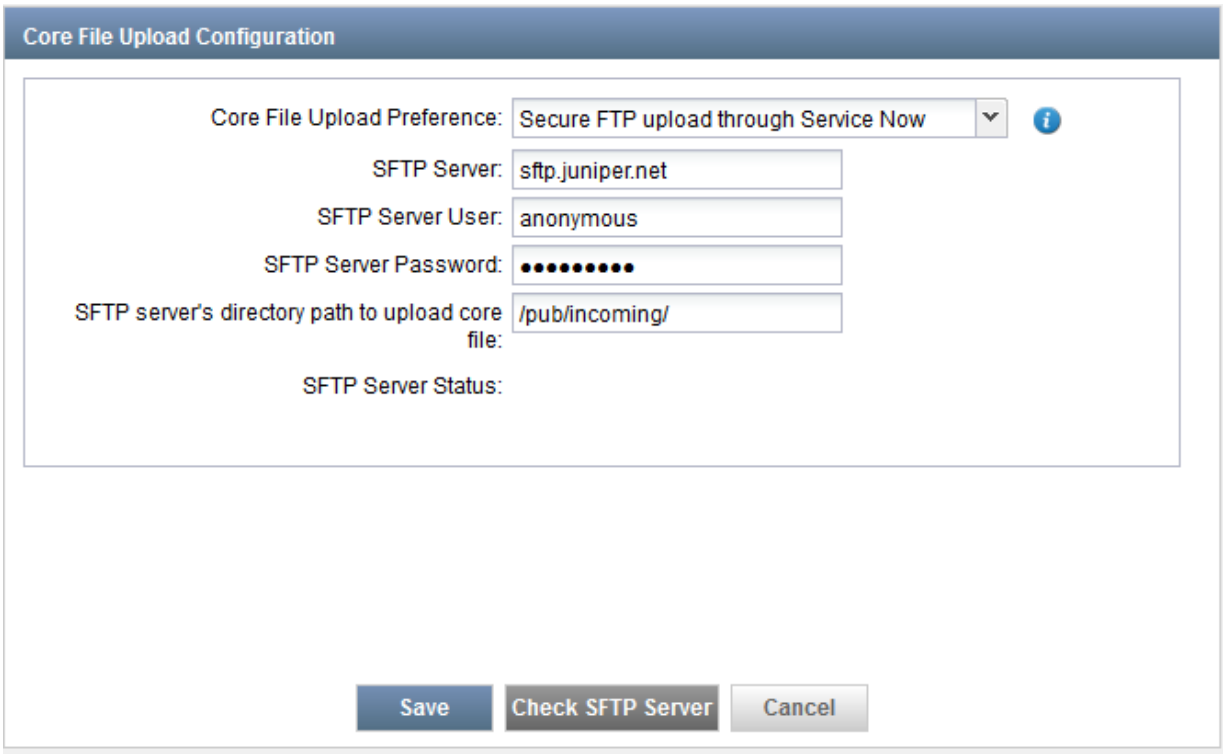
You cannot configure SFTP server to upload core files in an Offline mode.

To upload core files:

1. From the Service Now navigation tree, select **Administration** > **Global Settings**> **Core File Upload Configuration**.

   The Core File Upload Configuration page appears as shown in Figure 6 on page 85.

Figure 6: Core File Upload Configuration Page



2. Select the upload preference from the **Core File Upload Preference** drop-down list.

   The available options are:

   - **Disabled-Core Files uploaded manually**: If you select this option, Service Now does not upload core files to the FTP server. You have to manually upload the core files to the SFTP server.

- **Secure FTP upload through Service Now**: If you select this option, Service Now uploads the core files to the SFTP server after downloading the core files from a device.

3. Enter the required parameters in the respective fields.

4. Click **Submit**.

> **NOTE:** For Service Now operating in End Customer mode, these fields are disabled. In the End Customer mode, the values for all the fields are retrieved from the partner. The **Update Credentials** field is available to update the credentials from the associated Service Now partner.

5. Click **Check SFTP Server** to verify connectivity of Service Now with the SFTP server.

   The **SFTP Server Status** field displays **Success** if the Service Now is able to connect to the SFTP server.

RELATED DOCUMENTATION

Updating Core File Upload Configuration for an End Customer | 132

Directive File Overview

Junos Space Service Now creates off-box Juniper Message Bundle (JMB) by using a directive file (**directive.rc**). The directive file stores a list of devices for which Service Now can generate JMBs without using the AI-Scripts (off-box JMBs) installed on the devices.

Service Now provides a default directive file. The directive file is updated automatically to include support for new devices using updates from Juniper Support Systems (JSS). Starting in Service Now Release 16.1R1, Service Now provides options to manage the directive file so that off-box JMBs can be generated for devices newly supported by Service Now.

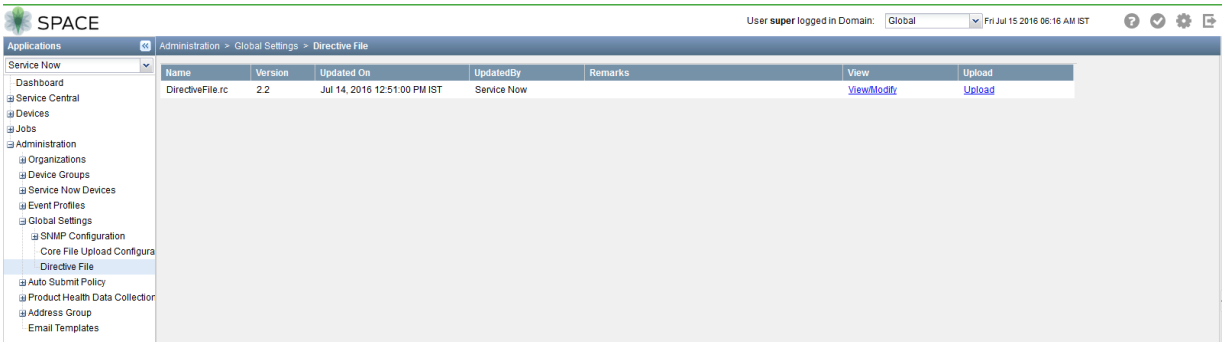
> **NOTE:** Service Now executes the RSI brief command on devices running subscriber management services instead of the normal RSI command to avoid impacting performance of device CPU.

For Service Now operating in Offline mode, Juniper Networks provides the directive file by e-mail, which can be manually uploaded to Service Now. Service Now operating in End Customer mode receives updates,

if any, from the Service Now partner once every 24 hours and the directive file is updated. Service Now does not verify the contents of the directive file that you upload, but only validates the version of the directive file. Therefore, we recommend that you do not modify the directive file.

You can view the directive file on the Directive File page (**Administration > Global Settings > Directive File**) as shown in Figure 7 on page 87.

Figure 7: Directive File Page



The Directive File page displays the following details:

- Name—name of the directive file
- Version—version of the directive file
- Updated On—date and time the directive file was last updated
- Updated by—entity that updated the directive file; the value is Service Now if the file is automatically updated by Service Now; otherwise, the username of the user who uploaded the directive file is listed
- Remarks—any remarks about the directive file
- View—link to view or modify the directive file
- Upload—link to upload a directive file

You can perform the following tasks from the Directive Files page:

- Update the directive file with the latest file available in JSS; see "Updating the Directive File in Junos Space Service Now" on page 88 for details
- Restore the directive file shipped with Service Now; see "Restoring the Default Directive File" on page 91 for details

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16.1R1, Service Now provides options to manage the directive file so that off-box JMBs can be generated for devices newly supported by Service Now

RELATED DOCUMENTATION

Generating an On-Demand Incident | 174

Updating the Directive File in Junos Space Service Now

NOTE: Service Now does not validate the contents of the directive file that you upload. Therefore, we recommend that you do not modify the directive file. If you want changes to the directive file, contact Juniper Networks for assistance.

Changes to a directive file are tracked by version number of the directive file. Service Now checks Juniper Support Systems (JSS) (in Direct or Partner Proxy mode) or the Service Now partner (in case of End Customer) once every 24 hours for updates to the directive file. Any change to the directive file is indicated by a change in the version number. If the version number of the directive file in JSS or Service Now partner is higher than the version number of the directive file in Service Now, Service Now fetches the directive file from JSS or Service Now partner and replaces the file in the Service Now database with the fetched file. To view the details and the content of the updated file on the Directive File page, see “Directive File Overview” on page 86.

You can also use the Refresh option provided on the Directive file dialog box to check for updates to the directive file in JSS or Service Now partner and fetch the updated directive file.

NOTE: Starting Service Now Release 17.1R1, **Update Directive File From Juniper Support System** check box available in the Advanced Settings task of the Global Settings menu provides an option to avoid updating the directive file in Service Now automatically when a newer version of the directive file is available in JSS.

To use the Refresh option:

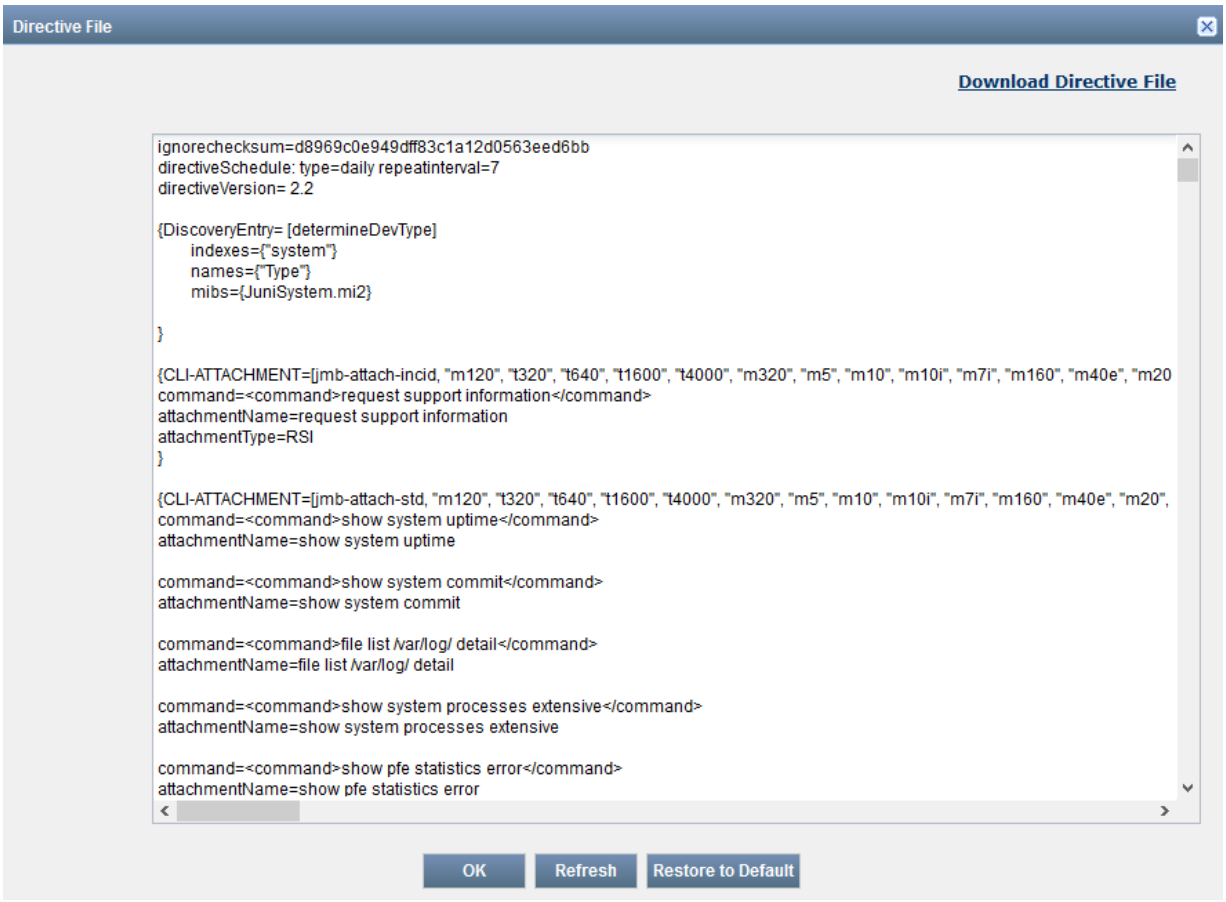
1. From the Service Now navigation tree, select **Administration > Global Settings > Directive File**.

   The Directive File page appears.

2. Click the **View/Modify** link in the View column.

   The Directive File dialog box appears as shown in Figure 8 on page 89.

Figure 8: Directive File Dialog Box



3. Click the **Refresh** button.

Servic Now replaces the current directive file with the latest file from JSS or Service Now partner.

Check the last updated date and time in the Updated On column and the version number in the Version column of the Directive File page to confirm that the directive file is updated. The directive file is updated only if the version of the file in JSS or Service Now partner is higher than that of the file in the Service Now database.

For Service Now operating in Offline mode, Juniper Networks provides the directive file. The directive file must be manually uploaded to Service Now.

Before you begin, store the directive file you receive on your local system.

To manually upload a directive file to Service Now:

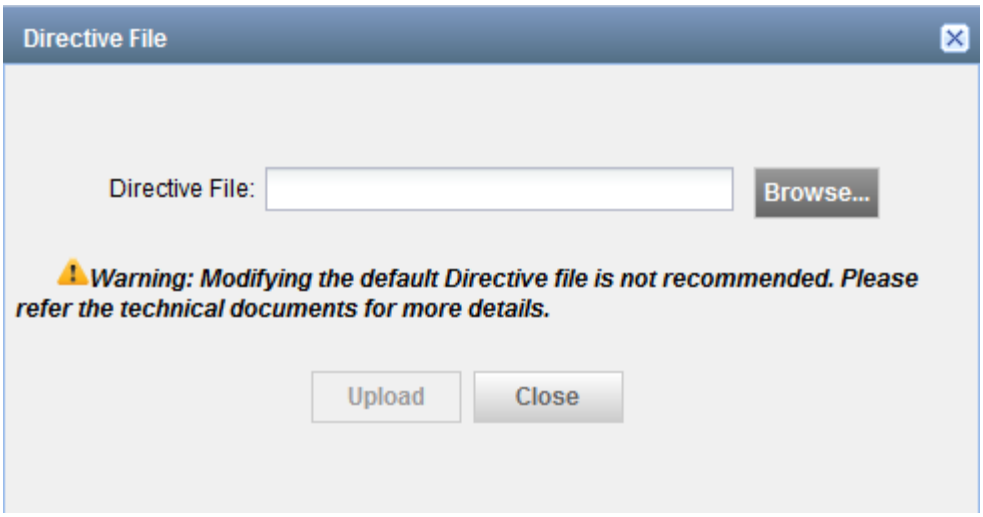
1. From the Service Now navigation tree, select **Administration > Global Settings > Directive File**.

   The Directive File dialog box appears.

2. Click the **Upload** link in the Upload column.

   The Directive File dialog box appears as shown in Figure 9 on page 90.

Figure 9: Directive File Upload Dialog Box



3. Click the **Browse** button to browse for the received directive file.

4. Click **Upload** to upload the directive file.

The received directive file is uploaded to Service Now.

5. Confirm that the received file is uploaded by checking the version number displayed on the Directive File page. The version number should reflect the version number on the directive file received from Juniper Networks or the Service Now partner.

Release History Table

Release	Description
17.1R1	Starting Service Now Release 17.1R1, **Update Directive File From Juniper Support System** check box available in the Advanced Settings task of the Global Settings menu provides an option to avoid updating the directive file in Service Now automatically when a newer version of the directive file is available in JSS.

Restoring the Default Directive File

Junos Space Service Now provides the Restore option to replace an updated or modified directive file with the default directive file shipped with Service Now.

To restore the default directive file shipped with Service Now:

1. From the Service Now navigation tree, select **Administration > Global Settings > Directive File**.

   The Directive File page appears.

2. Click the **View/Modify** link in the Modify column.

   The Directive File dialog box appears.

3. Click the **Restore to Default** button.

   Service now restores the current file with the default directive file.

Configuring Advanced Filter Settings

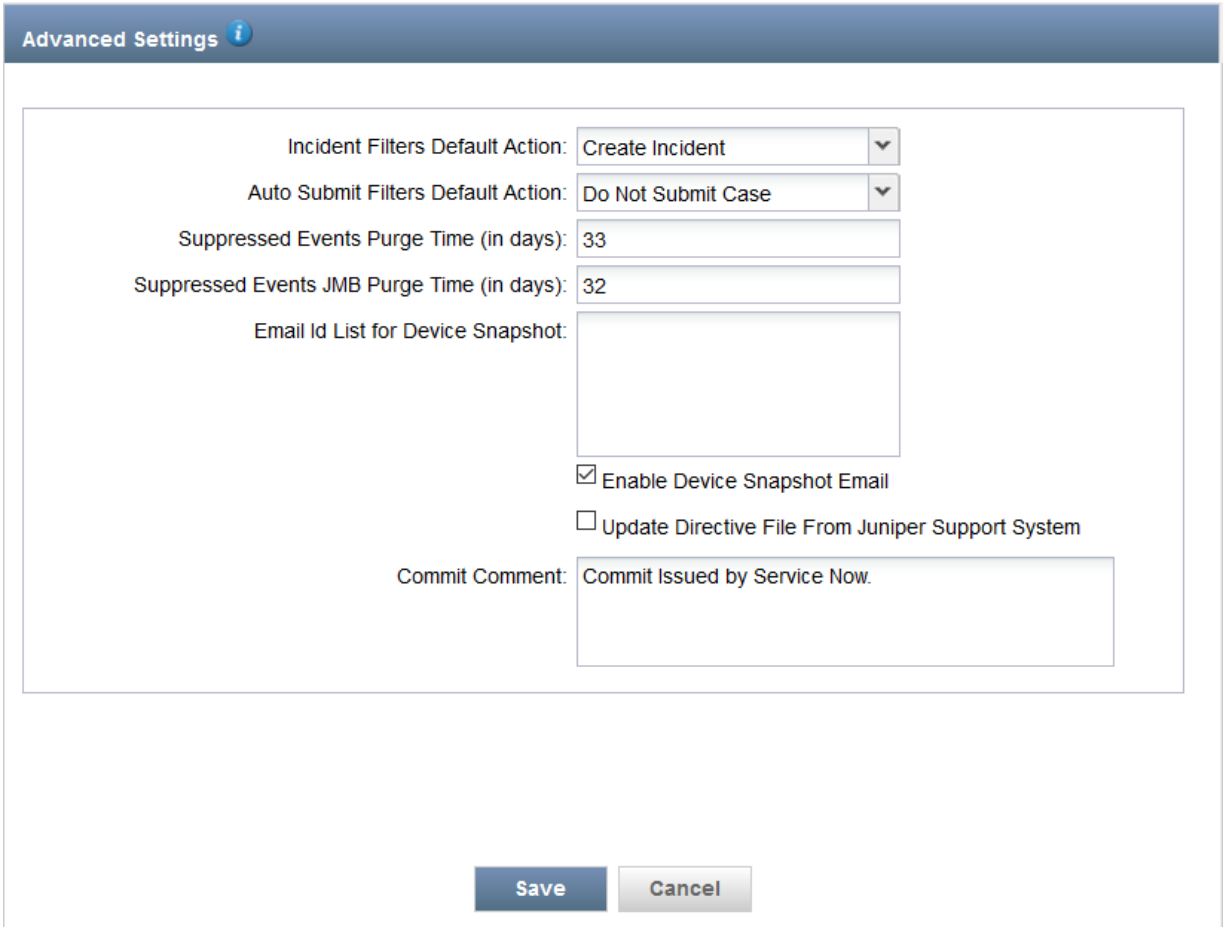
Advanced filter settings define the action that Service Now should take when a JMB or an incident does not match any of the defined incident or auto submit filters. You can define the advanced filter settings in the Global settings task.

To define advanced filter settings:

1. In the Service Now navigation tree, click **Administration > Global Settings > Advanced Settings**.

   The Advanced Settings page appears as shown in Figure 10 on page 92.

Figure 10: Advanced Settings Page



2. On the Advanced Settings page, configure values for parameters as follows: :

- Select a default action for incident filters in the **Incident Filters Default Action** drop-down list—Create Incident, Do not Create Incident.
- Select a default action for auto submit filters in the **Auto Submit Filters Default Action** drop-down list—Submit Case, Do Not Submit Case.
- Enter the number of days suppressed events can be stored in the Service Now database before they are deleted in the **Suppressed Events Purge Time (in days)** text box.

> **NOTE:** Whenever the suppressed events are purged or deleted, the associated JMBs are also purged or deleted. However, if suppressed JMBs are deleted, the suppressed events are not deleted.

- Enter the number of days suppressed JMBs can be stored in the Service Now database before they are deleted in the **Suppressed Events JMB Purge Time (in days)** text box.
- In the **Email Id List for Device Snapshot** field, enter the list of e-mail IDs of users to whom you want to send device snapshots by e-mail.

  If you do not configure any e-mail IDs, device snapshots are sent by e-mail only to the Super user. If you configure e-mail IDs, then device snapshots are sent by e-mail to only the configured e-mail IDs and not to the Super user.
- (Optional) Clear the **Enable Device Snapshot Email** check box to disable sending device snapshots as an email attachment to users.

  By default, this check box is selected and e-mail with device snapshots as attachment is sent to all e-mail IDs configured in the Email Id List for Device Snapshot text field or to the Super user if no e-mail ID is provided.
- (Optional) Clear the **Update Directive File From Juniper Support System** check box to avoid service Now from automatically updating the directive file..

  By default, the Update Directive File From Juniper Support System check box is selected and Service Now automatically updates the directive file when a newer version of the file is available in JSS or Service Now partner (in case of End Customer mode).

3. (Optional) Enter a generic comment while installing or uninstalling event profiles in the **Commit Comment** text box.

   The comment you enter in this text box appears as the default comment in the **Commit Comment** text box on the Install Event Profile and Uninstall Event Profile pages (**Administration > Service Now Devices > Device Operations**). If you do not add a comment, Service Now adds the following default comment: Commit Issued by Service Now.

   This comment is also used as the commit comment for the AI-Scripts configuration while uninstalling AI-Scripts configuration from a device before deleting the device from Service Now.

4. Click **Save** to save the changes.

   Service Now displays a confirmation message indicating that the changes are successfully saved.

CHAPTER 5

User Roles

User Roles and Permissions Overview | 97

Junos Space Service Now User Roles | 97

Junos Space Service Insight User Roles | 103

User Roles and Permissions Overview

Junos Space Network Management Platform provides role-based access control (RBAC). A user is allowed access to the Junos Space Network Management Platform and applications after authentication and authorization.

A Junos Space Super Administrator or User Administrator controls the workspaces that users can access, the system resources that a user can view and manage, and the tasks available to users within a workspace. RBAC is enforced in the Junos Space user interface navigation hierarchy by workspace, task group, and task. A user can access only those portions of the navigation hierarchy that are explicitly granted through access privileges. For more information about role-based access control, see the *Role-Based Access Control Overview* topic of the *Junos Space Network Management Platform User Guide* at Junos Space Documentation.

While Junos Space Platform allows creating users with custom permissions, it also has a set of predefined user roles. These predefined roles cannot be modified or deleted.

For information about predefined user roles in Junos Space Platform, see the Predefined Roles Overview topic of the *Junos Space Network Management Platform User Guide* at junos Space Documentation. For information about predefined user roles for Junos Space Service Now and Junos Space Service Insight, see the following:

RELATED DOCUMENTATION

Junos Space Service Now User Roles | 97

Junos Space Service Insight User Roles | 103

Junos Space Service Now User Roles

The Junos Space 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 allows creating users with custom permissions, it also has a set of predefined user roles. These predefined roles cannot be modified or deleted. Table 10 on page 98 lists the predefined roles available in Junos Space Service Now.

Table 10: Predefined Roles for the Service Now Application

Role	Workspace	Task Groups and Tasks
Service Now Admin	Administration	

Table 10: Predefined Roles for the Service Now Application *(continued)*

Role	Workspace	Task Groups and Tasks
		• **Incident Filters**: Create basic filter, create advanced filter, import incident filters, modify incident filters, delete incident filters, export incident filters, reorder incident filters, enable incident filters, disable incident filters, and assign incident filters to a domain • **Auto Submit Filters**: Create basic filter, create advanced filter, import auto submit filters, modify auto submit filters, delete auto submit filters, export auto submit filters, reorder auto submit filters, enable auto submit filters, disable auto submit filters, and assign auto submit filters to a domain • **Global Settings**: Manage directive file, configure an FTP server for uploading core files, manage SNMP traps, and configure Service Now partner certificates on a Service Now end customer, configure advanced settings • **Address Group**: Create address groups, associate address groups with devices, modify address groups, delete address groups, and assign address groups to domains • **Device Groups**: Create device groups, modify device groups, set a device group as the default device group, associate address groups with device groups, assign device groups to domains, and delete device groups from Service Now • **Service Now Devices**: Add devices to Service Now, export device inventory information, associate devices with autosubmit policies, associate devices with device groups, check FTP server configuration, configure RSI and log file collection on devices, create on-demand incidents, associate devices with address groups, export device information, install event profiles on devices, request Return Materials Authorisation (RMA), uninstall event profile from devices, view exposure of devices to known events, view incidents generated on Service Now, assign the Service Now devices to domains, and delete devices from Service Now • **Email Templates**: Modify default content of an Email template and restore the modified content of an Email template to its default content • **Event Profiles**: Add AI-Scripts bundles to Service Now, set an AI-Scripts bundle as the default AI-Scripts bundle in Service Now, delete AI-Script bundles, create event profiles, import event profiles, export event profiles to an XML file, push event profiles to devices, clone event profiles, set an event profile as the default profile, view events included in event profiles, view devices associated with event profiles, assign event profiles to domains, and delete event profiles from Service Now • **Auto Submit Policy**: Create autosubmit policies, export incident reports, modify autosubmit policies, change the dampening status of autosubmit policies, assign autosubmit policies to a domain, and delete autosubmit policies from Service Now • **Organization**: Add an organization to Service Now, add end customers to

Table 10: Predefined Roles for the Service Now Application *(continued)*

Role	Workspace	Task Groups and Tasks
		organizations, check the connection status of Service Now with Juniper Support System (JSS) or with a Service Now partner, modify organizations, associate address groups with organizations, delete organizations, update core file upload configuration, view information messages received from JSS, and assign organizations to domains • **Product Health Data Collection (PHDC)**: Configure PHDC, modify PHDC, delete PHDC, enable PHDC on devices, disable PHDC on devices, reschedule PHDC on devices, retry PHDC on failed devices, abort PHDC on devices, delete product health data (PHD) files, download product health data files, export information about product health data and devices
	Service Central	• **Incidents**: Create autosubmit policies, view end-customer cases in Case Manager, update end-customer cases, export JMB to HTML, export incident summaries to Excel, assign an owner to incidents, view end-customer cases created in Service Now, flag incidents to users, submit cases to JSS or a Service Now partner, view KB articles related to an incident, delete incidents, view tech support cases in Case Manager, update tech support cases, upload core files to JSS, Upload attachments to cases, and view JMB associated with an incident • **Information**: View iJMBs, export iJMBs to HTML, delete iJMBs, assign messages received from JSS to connected members, assign ownership to messages, delete messages, Flag messages to users, and scan devices for impact based on messages received from JSS • **View Tech Support Cases**: View cases in Case Manager, update cases, and upload text or binary attachments to cases • **View End Customer Cases**: View end-customer cases in Case Manager and Update end-customer cases • **Device Analysis**: Delete BIOS validations, export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • **JMB Errors**: Download error JMBs and delete error JMBs • **Suppressed Events**: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • **Notifications**: Create notifications, edit notification filters and actions, copy notifications, delete notifications, enable or disable notifications, and assign notifications to domains

Table 10: Predefined Roles for the Service Now Application *(continued)*

Role	Workspace	Task Groups and Tasks
Service Now Read Only	Administration	**Service Now Devices**: Export event profiles, export devices, view exposure of devices to known events, and create on-demand device snapshots, export information about product health data and devices, download product health data files
	Service Central	• **Incidents**: Export a JMB in HTML format, view JMBs, export incident summary to Excel, and view tech support and end-customer cases in Case Manager • **JMB Errors**: Download error JMBs • **Tech Support cases**: View tech support cases in Case Manager and update cases • **Information**: View iJMBs, export iJMBs to HTML and scan devices for impact based on messages received from JSS • **Device Analysis**: Export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • **Suppressed Events**: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • **Notifications**: Create notifications • **End-customer cases**: View end-customer cases in Case Manager

Table 10: Predefined Roles for the Service Now Application *(continued)*

Role	Workspace	Task Groups and Tasks
Service Now Unrestricted User	Administration	**Service Now Devices**: Export devices, view exposure of devices to known events, create on-demand device snapshots, and export event profiles, export information about product health data and devices, download product health data files
	Service Central	• **Incidents**: Export JMBs to HTML, view JMBs, export incident summaries to Excel, view tech support and end-customer cases in Case Manager, update tech support and end-customer cases, delete incidents, submit cases to JSS, assign ownership to incidents, and flag incidents to users • **Tech Support cases**: View tech support cases in Case Manager and update cases • **JMB Errors**: Download error JMBs and delete error JMBs from Service Now • **Suppressed Events**: Delete suppressed JMBs, create incidents for the suppressed JMBs, view the suppressed JMBs • **View Tech Support Cases**: View tech support cases in case manager, update cases in case manager • **Information**: Assign owners to messages received from JSS, flag messages received from JSS to users, delete messages received from JSS, assign messages received from JSS to end customers, export iJMBs to HTML, view iJMBs, and delete iJMBs from Service Now • **Device Analysis**: Delete BIOS validations, export BIOS validations to Excel, view device health data, and view devices on which PHD are collected, export information about product health data and devices, download product health data files • **View End Customer Cases**: View end-customer cases in Case Manager and update end-customer cases • **Notifications**: Create notifications, edit filters and notifications, copy notifications, enable or disable notifications, assign notifications to domains, and delete notifications

To create and manage users, on the Junos Space Network Management Platform GUI, select **Network Management Platform** > **Role Based Access Control** > **User Accounts**. The User Accounts page lists the existing users. Use this page to create and assign roles to Service Now and Service Insight users.

For information about creating users, see*Creating User Accounts in Junos Space Network Management Platform* in the *Junos Space Network Management Platform User Guide* available at https://www.juniper.net/documentation/en_US/release-independent/junos-space/index.html.

RELATED DOCUMENTATION

Service Central Overview

Service Now Administration Workspace Overview | 35

Junos Space Service Insight User Roles | 103

Junos Space Service Insight User Roles

The Junos Space 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 allows creating users with custom permissions, it also has a set of predefined user roles. These predefined roles cannot be modified or deleted. See Table 11 on page 103 for the list of predefined user roles available in Service Insight. All the roles are applicable in the Insight Central workspace of the Service Insight application.

Table 11: Predefined Roles for the Service Insight Application

Role	Task Groups and Tasks
Service Insight Administrator	• **Exposure Analyzer**: View PBNs that can impact devices, generate EOL reports, and generate PBN reports • **EOL Reports**: Regenerate EOL reports, export EOL reports, and delete EOL reports from Service Insight • **PBN Reports**: Regenerate PBN reports, export PBN reports, and delete PBN reports • **Targeted PBNs**: Scan for impact, flag PBNs to users, e-mail PBN to users, assign owners to PBNs, and delete PBNs from Service Insight • **Notifications**: Create notifications, edit filters and actions in notifications, copy notifications, delete notifications, enable or disable notifications, and assign notifications to domains
Service Insight Read Only User	• **Exposure Analyzer**: View PBNs that can impact devices • **EOL Reports**: Export EOL reports in Excel format • **PBN Reports**: Export PBN reports in Excel format • **Targeted PBNs**: Scan devices for that are impacted by the PBNs

Table 11: Predefined Roles for the Service Insight Application *(continued)*

Role	Task Groups and Tasks
Service Insight Unrestricted User	• **Exposure Analyzer**: View PBNs that can impact devices, generate EOL reports, and generate PBN reports • **EOL Reports**: Regenerate EOL reports, export EOL reports, and delete EOL reports • **PBN Reports**: Regenerate PBN reports, export PBN reports, and delete PBN reports • **Targeted PBNs**: Scan for impact, flag PBNs to users, e-mail PBNs to users, assign owners to PBNs, and delete PBNs from Service Insight • **Notifications**: Create notifications, edit filters and actions in notifications, copy notifications, delete notifications from Service Insight, enable or disable notifications, and assign notifications to domains

To create and manage users, on the Junos Space Network Management Platform GUI, select **Network Management Platform** > **Role Based Access Control** > **User Accounts**. The User Accounts page lists the existing users. Use this page to create and assign roles to Service Now and Service Insight users.

For information about creating users, see*Creating User Accounts in Junos Space Network Management Platform* in the *Junos Space Network Management Platform User Guide* available at https://www.juniper.net/documentation/en_US/release-independent/junos-space/index.html.

RELATED DOCUMENTATION

User Roles and Permissions Overview | **97**

Insight Central Overview

Junos Space Service Now User Roles | **97**

6

CHAPTER

Service Now End Customer-Partner Communication

Service Now End Customer–Partner Communication Overview | **107**

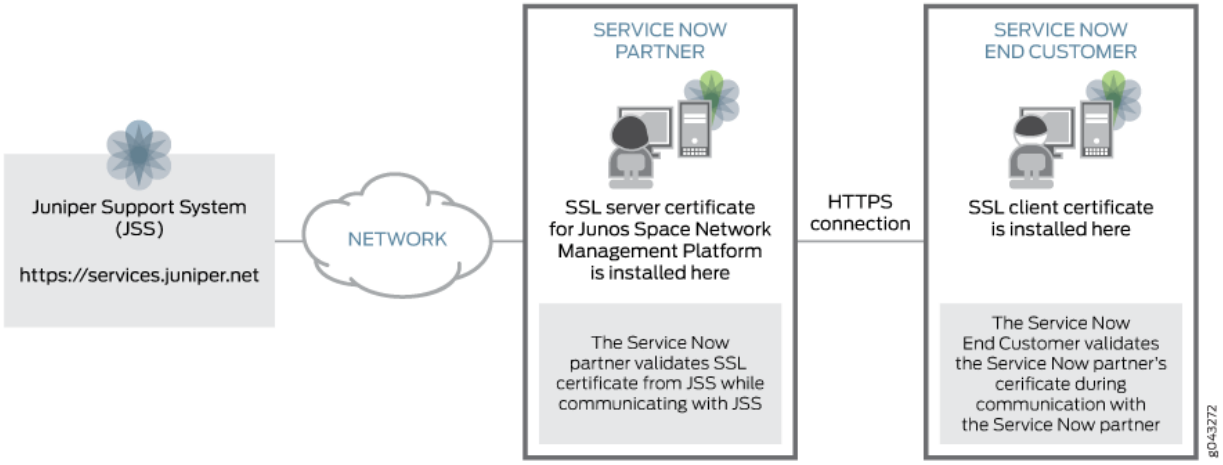
Installing the SSL Certificate on a Service Now End Customer | **113**

Service Now End Customer–Partner Communication Overview

A Service Now end customer establishes connection with a Service Now partner by using the HTTPS protocol. When a Service Now end customer initiates a request for communication with the Service Now partner, the Service Now partner provides a Secure Sockets Layer (SSL) certificate for the Service Now end customer to validate. The Communication between the Service Now partner and Service Now end customer is established after the Service Now end customer validates the certificate.

Figure 11 on page 107 depicts the communication between a Service Now partner with a Service Now End Customer and Juniper Support Systems (JSS) by using an SSL certificate.

Figure 11: Service Now Partner Communicating with a Service Now End Customer and JSS Using SSL Certificate



For information about using SSL certificates, see Certificate Management Overview.

By default, Junos Space Service Now uses a self-signed SSL certificate, provided by the Junos Space Network Management Platform, to validate connections between a Service Now partner and Service Now end customers. However, from Service Now Release 14.1R3, a Service Now partner can use a custom SSL certificate instead of the default self-signed certificate to secure communication with Service Now end customers.

To secure the communication between a Service Now partner and Service Now end customer, perform the following tasks:

1. Generating CSR by Service Now Partner | 108
2. Obtaining Signature of a Certificate Authority | 111

3. Uploading the Certificate to Service Now Partner | **111**
4. Obtaining the Intermediate Certificate (key) for Establishing Credibility of the SSL Certificate | **111**
5. Obtaining SSL Certificate of the Service Now Partner | **112**

Generating CSR by Service Now Partner

To install a custom SSL certificate on the Service Now partner, you must first generate a Certificate Signing Request (CSR):

To generate a CSR:

1. Log in to the Junos Space Appliance.

   The Junos Space Settings Menu Is displayed.

2. Type **7** if the Junos Space Appliance is a virtual appliance or type **6** if the Junos Space Appliance is a hardware appliance to access the SSH shell.

3. Change the directory to **/etc/pki/tls**.

   ```
   [root@host] cd /etc/pki/tls
   ```

4. Open the **openssl.cnf** file and comment out all instances of **subjectAltName=${ENV::SAN}**.

   ```
   <snip>
   # subjectAltName=${ENV::SAN}
   <snip>
   ```

5. Save the file.

6. Generate a private key by executing the following command:

   ```
   server $ openssl genrsa -des3 -out server.key 1024
   Generating RSA private key, 1024 bit long modulus
   ......++++++
   .............++++++
   e is 65537 (0x10001)
   ```

```
      Where 1024 is the length of the key in bits and server.key is the name of
      the key file.
```

7. Enter a pass phrase for the private key.

```
sever $  Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

8. Generate a signing request using the private key and password.

   You are prompted to provide your details such as the state or province to which you belong, your locality, email address and so on.

```
server $ openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:Sydney
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Juniper
Organizational Unit Name (eg, section) []:AS
Common Name (e.g. server FQDN or YOUR name) []:he-man
Email Address []:fred@juniper.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:fred1234
An optional company name []:
server $
```

   After this step is executed, you can find the following encrypted files in the **/etc/pki/tls** folder:

- **server.key**—The private key for the SSL certificate.

  The following is a sample of the **server.key** file obtained by using the **cat server.key** command:

```
server $ cat server.key
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,019649A2E4BBCC4C

uKKzDLcMrBpuYDkxSl6epQqoScvcYnJvTM5kaJKNNxVrUarYA16JYFszBOEpqCjr
AV7Ln6hg8Jl+UPEbrZPvXVED29qvM4tp1SDwKwuLs+IRWsON9ee2TSmVubCEOAc7
aA8jg7kzubCktF3y+8/lM3yf+IWMy4EdWBXwTjMBO22kjU5KGwyznQeCsN2HtOLp
WvFOFDQHgxougL0qfF7pkDsVby5bKv74OT+ju/On6HtLf8IUfZDh/Xui/scsoKeb
8eJnNKNOldYAtU+eyNwkmP1o9j8Ly/GeeiOOamMFaDpO1WuMQLmEH8En3tVIULrD
WZ2Ly0U9+d6Jl6f7LXXIEcBcH0eOOC3pp7Bq4zlkO/2WPq5FmcM9OmZZdeC2ZeYP
fNzBk2lZVVDAM89ggNlRNsm6FG9F6kkfczjBOSvawhBs7AgTDzty5J279uTGIyol
lCVXbijo9+KR3INX3nWatYYR7T7MUG1Yma/MbCg2dWAPR6iwYWY3w6VD51BIGNCP
po42YOH4yLvT8OuVzkpQ8z9tjukO5ZAR6E8fWEdiYBbPIhfEBxc7WVUBdPE/OQaj
8FuyLnzY5iCxYltkyWhtXntX32NrHJdJp6A8HfJf/v3ZnJ8FRHrNXtALcENVkgit
iCgmsGr5zwThiJqdSp6Xd4YpJrws5baTGRNjOrhfunGyEebhYmsQVKZpuXYM/YuV
5/Nqd3Hdmx58hWXViOCm7+HUlRFRCu+JBhBLOJ9rBzaDVAFRqNtkMkFlwHKQ6u9K
ly+qgO7gT8jYIWGfKsB70QdMF+MntA+SvD5bfoUd6CY=
-----END RSA PRIVATE KEY-----
```

- **server.csr**—The CSR file to be signed by a Certificate Authority (CA).

  The following is a sample of the **server.csr** file obtained by using the **cat server.csr** command:

```
server $ cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwfTELMAkGA1UEBhMCQVUxDDAKBgNVBAgTA05TVzEPMA0GA1UE
BxMGU3lkbmV5MRAwDgYDVQQKEwdKdW5pcGVyMQswCQYDVQQLEwJBUzEPMA0GA1UE
AxMGaGUtbWFuMR8wHQYJKoZIhvcNAQkBFhBmcmVkQGp1bmlwZXIubmV0MIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCjA2megTM4/9iP9I56iNqmKmROQYfPwHLn
pW7BWq1Dikzn8BqM6cFeMa1vUpRntiPJRNbUjGZPbfa3cwZEy/vgy3MyTALFj9Zy
7tkpUIdlQn2Khw47mEcaixkEec5PxOUZm3Af1kKcMtIzajxxyVRs6cr6xLy0Bqew
1TA+3Xj6PwIDAQABoBkwFwYJKoZIhvcNAQkHMQoTCGZyZWQxMjM0MA0GCSqGSIb3
DQEBBQUAA4GBAJjxApGFYAFfUl1x0osdoGzedRkrVmR5693+hOEtI01n0z7ONCVu
ixOin4dH0SDipNPgfZwQ0jx6wyVGx/b6wWpMxBTrvhxH1EiCgR9pP0U63eMZsyEI
3RoU+7KeRTxxtXbRYUx0EHGPDOHSgiShbjVc2uAPXijSRlutI3sViTJ2
-----END CERTIFICATE REQUEST-----
```

Obtaining Signature of a Certificate Authority

The Service Now partner should get the **server.csr** file signed by a Certificate Authority (CA); for example, GeoTrust®, by contacting the CA. A signed certificate has the **.der** or **.pem** extension.

> **NOTE:** Service Now supports signed certificates in the x.509 format only. We recommend that while requesting a CA to sign your certificate, specify that you need the signed certificate in the x.509 format.

After you receive the signed certificate, save it on your local system.

Uploading the Certificate to Service Now Partner

The signed **server.csr** file should be uploaded to the Junos Space Platform on which the Service Now partner is installed.

For information about uploading custom SSL certificate to Junos Space Platform, refer to Installing Custom SSL Certificate on Junos Space Server.

Obtaining the Intermediate Certificate (key) for Establishing Credibility of the SSL Certificate

Download the certificate key from the website of the CA from whom you obtained the signature for the SSL certificate; for example, https://www.geotrust.com/resources/root-certificates/ is the website of GeoTrust®.

Ensure that you select the appropriate root certificate and upload the root certificate obtained from the CA to the Junos Space Platform by using the **Administration > CA/CRL Certificates** navigation path of the Junos Space Platform GUI. For more information, see Certificate Management Overview.

Obtaining SSL Certificate of the Service Now Partner

To secure communication with the Service Now partner, a Service Now end customer should obtain and install the SSL certificate from the Service Now partner.

> **NOTE:** The procedure to obtain SSL certificate of a Web server varies from one browser to another.

To obtain the SSL certificate of the Service Now partner using Mozilla Firefox Web browser:

1. Open Mozilla Firefox Web browser and enter the URL to access the Service Now partner.
2. On the web browser, click the padlock present before the URL.

   A dialog box with the information about the identity and security of the Service Now partner's Web site appears.
3. Click **More Information**.

   The Page Info dialog box appears.
4. Click **Security > View Certificate** on the Page Info dialog box.

   The Certificate Viewer dialog box appears displaying the SSL certificate used by the Service Now partner.
5. Click the **Details > Export** tab on the Certificate Viewer to export the SSL certificate.

   The Save To dialog box of the web browser appears.
6. Save the certificate on your local system.

   Ensure that the certificate is an X.509 certificate (***.pem**).

To obtain the SSL certificate of the Service Now partner using CLI:

1. Connect to the Virtual IP (VIP) node of the Junos Space cluster on which the Service Now partner is installed and configured.
2. Type **7** if the Junos Space Appliance is a virtual appliance or type **6** if the Junos Space Appliance is a hardware appliance to access the SSH shell.
3. Type the following from the command line:

```
server $ echo "" | openssl s_client -connect <hostname>:443 | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p'  > cert.pem

      where <hostname> is the hostname of the Service Now partner.
```

SEE ALSO

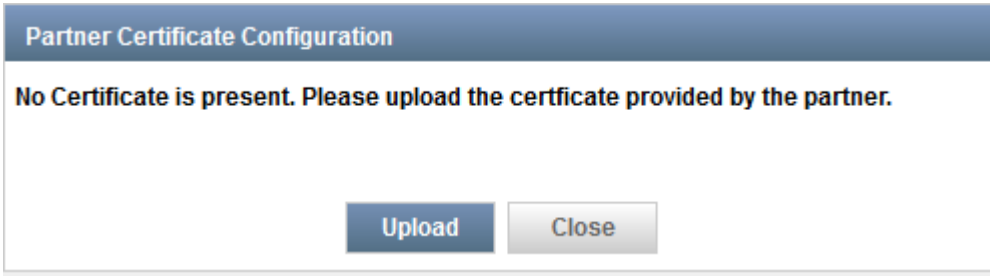
Installing the SSL Certificate on a Service Now End Customer | 113

Installing the SSL Certificate on a Service Now End Customer

To install the SSL certificate obtained from Service Now partner on a Service Now end customer:

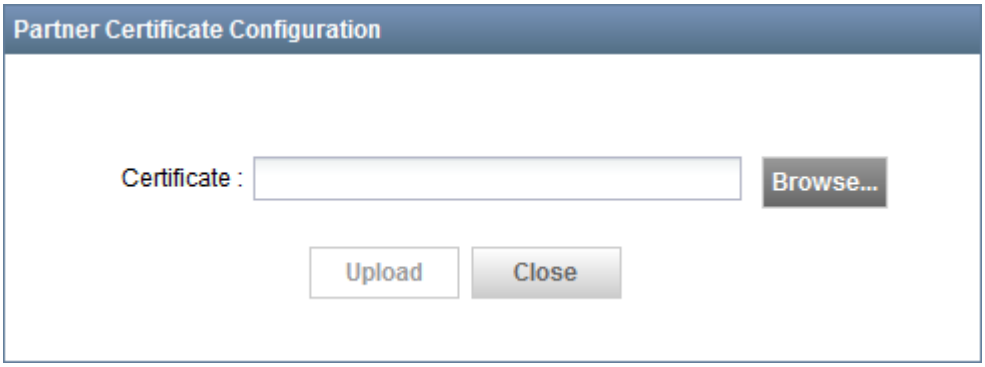
1. From the Service Now navigation tree, select **Administration** > **Global Settings** > **Partner Certificate Configuration**.

   The Partner Certificate Configuration page appears. This page displays the certificates currently used by Service Now end customer. If the Service Now end customer does not have any certificate, this page displays the option to upload a certificate.



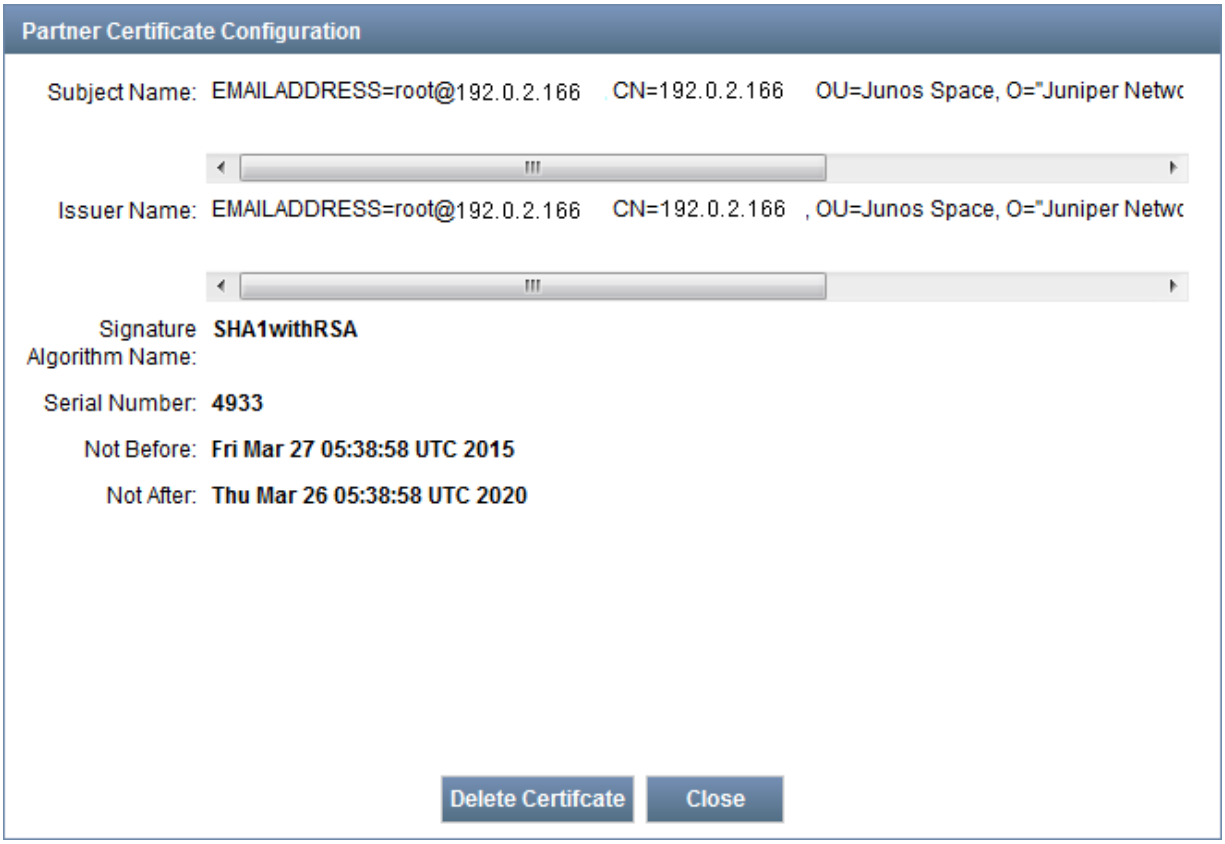
2. Click Browse to navigate and locate the certificate in your file system and then and then click **Upload**.

The Service Now GUI displays the option to browse and upload the certificate.



3. Click **Upload**.

   The certificate is uploaded and displayed in the Partner Certificate Configuration page.



RELATED DOCUMENTATION

Certificate Management Overview

7

CHAPTER

Configuring and Managing Organizations

Service Now Organizations Overview | **119**

Adding an Organization to Service Now | **122**

Adding an End Customer to Service Now Configured in Partner Proxy Mode | **125**

Modifying Organization Parameters | **128**

Deleting an Organization | **129**

Testing the Connection to JSS | **130**

Running an Organization in Test Mode | **131**

Updating Core File Upload Configuration for an End Customer | **132**

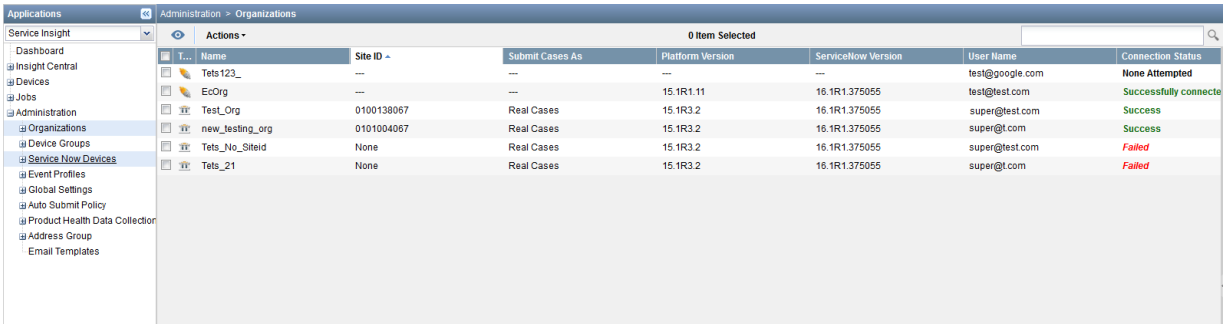
Viewing Messages Assigned to an End Customer | **132**

Service Now Organizations Overview

An organization in Junos Space Service Now represents a unique site ID in the Customer Relationship Manager (CRM) of the Juniper Support Systems (JSS). JSS identifies a Service Now application by using the site ID of the organization configured on the Service Now application. An organization is configured on Service Now by providing a site ID and credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks when Service Now is operating in Direct or Partner Proxy mode or by Service Now partner when Service Now is operating in the End Customer mode. When Service Now submits incidents for creating cases, the cases are created and associated with the site ID of the organization configured on Service Now.

You can view organizations configured in Service Now on the Organizations page (**Administration > Organizations**) as shown in Figure 12 on page 119.

Figure 12: Organizations Page



A Service Now partner can manage multiple organizations using a single Service Now installation. This is done by dividing the network into multiple logical customer sites and assigning each customer site to an organization. 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 "Service Now Device Groups Overview" on page 137.

For more information about creating device groups, see "Creating a Device Group" on page 138.

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

Table 12 on page 120 describes the fields displayed in the tabular view of the Organizations page and in the **Organizations Details** dialog box.

Table 12: Organization Column Descriptions

Column Name	Description
Name	Name of the organization.
Site ID	ID of the Customer Site in the Customer Relationship Manager (CRM) of JSS.
Submit Cases As	Specifies whether the cases from a production environment should be submitted to JSS as a real case or a test case. 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.
Platform Version	Version of Junos Space Network Management Platform used. In a Service Now partner, for an end-customer organization, this field displays the version of Junos Space platform used by the end customer.
Service Now Version	Version of Service Now used. In a Service Now partner, for an end-customer organization, this field displays the version of Service Now used by the end customer.
User Name	Username to identify the user for communication with the JSS while creating cases or checking updates. You do not need to enter a username or password if Service Now is operating in the offline mode.
Connection Status	Status of the connection between Service Now and JSS or Service Now partner. Possible values: Successful or Failed
JMB Filter Level (Only visible in the Detail Summary dialog box, which opens when you double-click the organization)	Filter defining the extent of device information in a JMB to be shared with JSS. Possible values: • Do not send Device Snapshots—Does not send device snapshots to JSS • Send all information except configuration—Sends all device information except the configuration information • Send all information with IP Addresses overwritten—Sends all device information with IP addresses overwritten by asterisks • Send all information—Sends all device information. • Only send list of features used—Sends only the device configuration information **NOTE:** The Only send list of features used option is applicable for device snapshots or information JMBs (iJMBs) only.

NOTE: Starting in Service Now Release 16.1R1, you can use the Platform Version and Service Now Version fields on the Organizations page to view versions of Network Management Platform and Service Now being used.

Associated Actions

You can perform the following actions related to organizations:

- Add an organization to Service Now; see "Adding an Organization to Service Now" on page 122 for details.
- Add an end customer to a Service Now partner; see "Adding an End Customer to Service Now Configured in Partner Proxy Mode" on page 125 for details.
- View organizations (including end-customer organizations in Partner Proxy mode) configured in Service Now.
- Modify the parameters of an organization; see "Modifying Organization Parameters" on page 128 for details.
- Configure an organization to submit cases as test case; see "Running an Organization in Test Mode" on page 131 for details.
- Test connectivity to JSS or Service Now partner; see "Testing the Connection to JSS" on page 130 for details.
- Delete an organization from Service Now; see "Deleting an Organization" on page 129 for details.
- Associate an organization with an address group; see "Associating Devices with an Address Group From the Organizations Page" on page 338 for details.
- Update core file upload configuration for a Service Now end customer; see "Updating Core File Upload Configuration for an End Customer" on page 132 for details.

  NOTE: This action is available only for an end customer on a Service Now partner setup.

- View messages assigned to end customers; see "Viewing Messages Assigned to an End Customer" on page 132 for details.

  NOTE: This action is available only for an end customer organization on a Service Now partner setup.

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16.1R1, you can use the Platform Version and Service Now Version fields on the Organizations page to view versions of Network Management Platform and Service Now being used.

RELATED DOCUMENTATION

Service Now Modes | 36

Service Now Global Settings Overview | 69

Service Now Address Group Overview | 333

Adding an Organization to Service Now

An organization in Service Now represents a unique site ID in the Customer Relationship Manager (CRM) of Juniper Support Systems (JSS).

An organization is configured on Service Now by providing a site ID and credentials (username and password) for the site ID. The site ID, username, and password are provided by Juniper Networks for operating Service Now in Direct and Partner Proxy modes. For operating Service Now in End Customer mode, the Service Now partner provides the username and password to configure an organization.

A user should have Service Now administrator privileges to add an organization to Service Now.

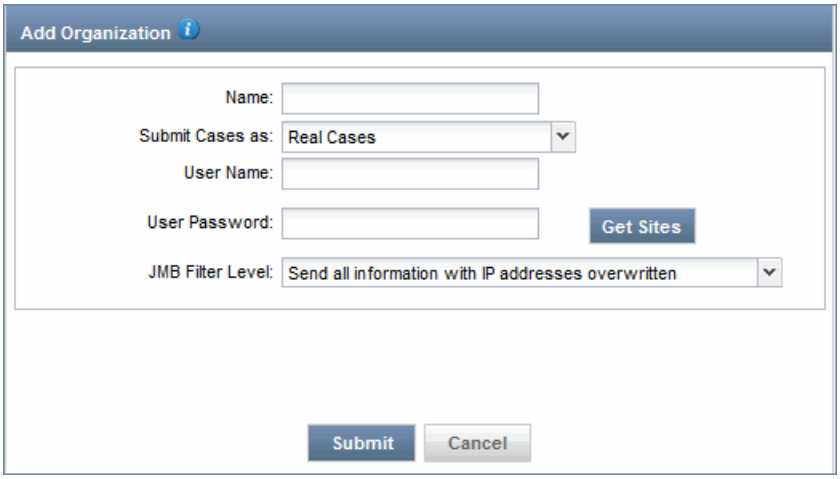
NOTE: In End Customer mode, you can add only one organization.

To add a Service Now organization:

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

   The **Add Organization** dialog box appears.

Figure 13: Add Organization Dialog Box



2. Enter the organization parameters in the provided fields. For a detailed description of these fields, see Table 13 on page 123.

Table 13: Description of Fields on the Add Organization Page

Name	Description	Range/Length	Default
Name	Name of the organization	maximum 64 characters are allowed.	
Submit cases as	Specifies whether cases from this organization should be submitted as real cases or test cases. The synopsis of a test case submitted to JSS or Service Now partner is appended with [Test Mode].	The values are: • Real cases • Test cases	Real Cases
User Name	Name used to identify the user in JSS while creating cases, and checking for updates to existing cases. You do not need to enter a username or password if Service Now is in the Offline mode.	128 characters; should be in the e-mail address format. Characters can include alphabets, numbers, and the following special characters: ., -, _, and +.	

Table 13: Description of Fields on the Add Organization Page *(continued)*

Name	Description	Range/Length	Default
User Password	Password for the username required for communicating with JSS or Service Now partner. You do not need to enter a username or password if Service Now is in the Offline mode.	32 characters	
Get Sites (button)	Identifier of a site in the Customer Relationship Manager(CRM) of JSS. 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 Service Now operating in the End Customer mode.	80 characters	
JMB Filter Level	The device configuration information in JMBs to be shared with JSS: • Do not send Device Snapshots—Does not send device snapshots to JSS • Send all information except configuration—Sends all device information except the configuration information • Send all information with IP Addresses overwritten—Sends all device information with IP addresses overwritten by asterisks • Send all information—Sends all device information. • Only send list of features used—Sends only the device configuration information **NOTE:** The Only send list of features used option is applicable for device snapshots or information JMBs (iJMBs) only.	–	Send all information with IP addresses overwritten

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

3. Click **Submit**.

Service Now saves the organization and returns to the Organization page.

RELATED DOCUMENTATION

Service Now Global Settings Overview | 69

Junos Space Service Now Modes

Adding an End Customer to Service Now Configured in Partner Proxy Mode

Junos Space Service Now that is operating in the Partner Proxy mode (referred to as Service Now partner) can manage multiple end customers over a secure HTTPS connection. In a Service Now partner, end customers are referred to as connected members. For a Service Now partner to communicate with an end customer, the Service Now application at the end-customer location (referred to as Service Now end customer) should have an organization configured on it. . The Service Now partner provides the username and password for configuring the organization in the Service Now end customer. For information about End Customer mode, see “Service Now Modes” on page 36.

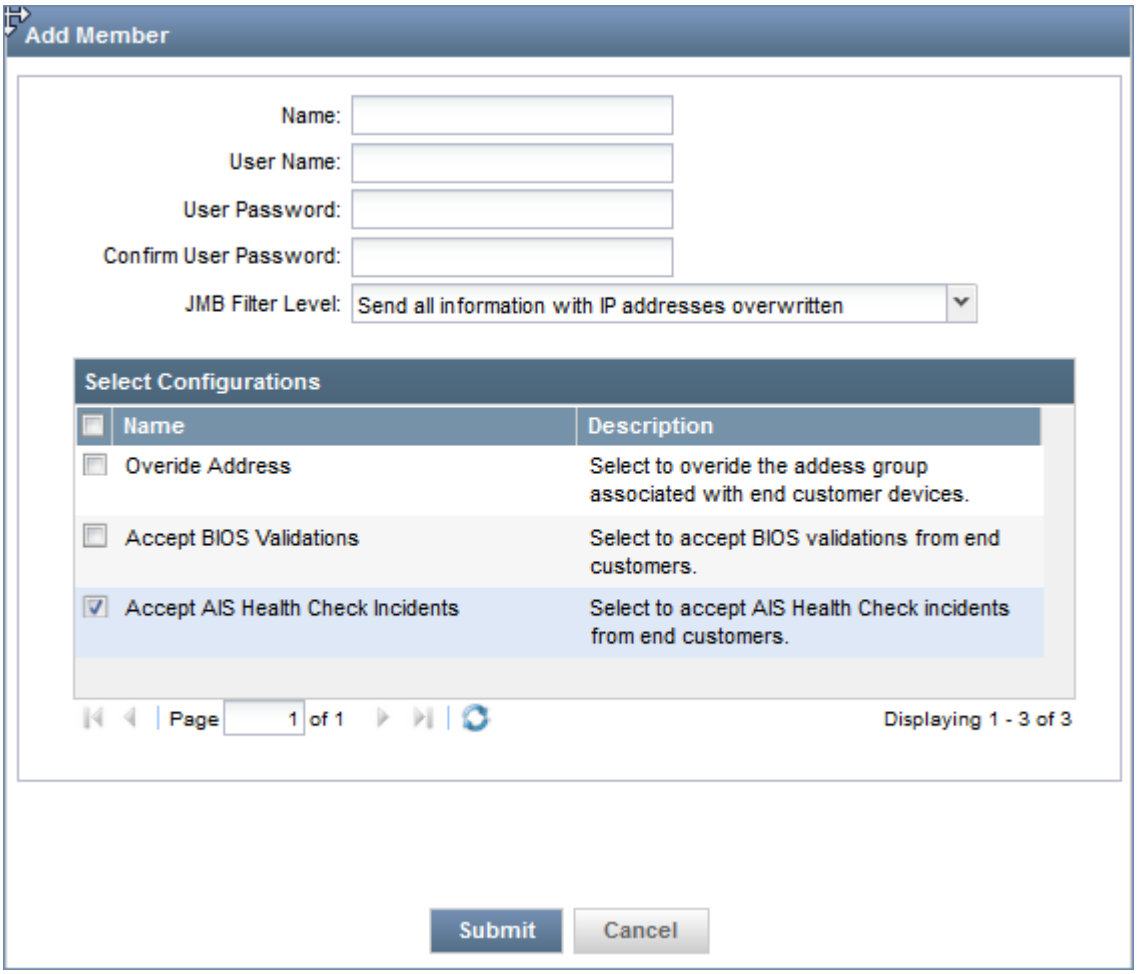
NOTE: An end customer can be added to a Service Now partner only after a valid organization is created in the Service Now end customer.

To add an end customer to Service Now configured in Partner Proxy mode:

1. From the Service Now navigation tree, select **Administration** > **Organization** > **Add Member**.

   The **Add Member** dialog box appears as shown in Figure 14 on page 126.

Figure 14: Add Member Dialog Box



2. In the **Name** filed, enter a name for the Service now end customer.

   The name must contain only alphanumeric characters (a-z, A-Z, 0-9). It cannot contain special characters such as underscores (_), spaces, or hyphens (-). The maximum number of characters allowed is 64.

3. In the **User Name** field, enter a username for the Service Now end customer.

   The end customer should use this username when submitting cases to the Service Now partner.

   The username must be in the user@example.com format.

4. In the **User Password** field, enter a password for the username.

5. In the **Confirm User Password** field, enter the same password for confirmation.

6. On the **JMB Filter Level** drop-down menu, select one of the following values to specify the information in a Juniper Message Bundle (JMB) that can be shared with the Service Now partner and Juniper Support Systems (JSS):

   - **Do not send Device Snapshots**—Does not send device snapshots to JSS
   - **Send all information except configuration**—Sends all device information in a JMB except the device configuration information
   - **Send all information with IP Addresses overwritten**—Sends all the device information; however, the IP addresses associated with the device are overwritten with asterisks (*)
   - **Send all information**—Sends all the device information
   - **Only send list of features used**—Sends parameters configured without values assigned to the parameters

     NOTE: The Only send list of features used option is applicable for device snapshots or information JMBs (iJMBs) only.

7. (Optional) Under **Select Configuration**, configure options as follows:

   - Select **Override Address** to override address group associated with end-customer devices. Overriding address groups of end customers allows a Service Now partner to send Return Materials Authorization (RMA) incidents of an end customer to JSS using the ship-to address associated with the device by the Service Now partner.
   - Select **Accept BIOS Validations** to accept BIOS data from a Service Now end customer for validation.

     If a Service Now partner does not select this check box, the **Configure BIOS Validation** option on the Actions list of Service Now devices is disabled on the Service Now end customer.

     NOTE: Starting Service Now Release 15.1R1, the Accept BIOS Validations check box is provided on the Add Member Dialog Box of a Service Now partner to accept or reject BIOS data from Service Now end customers for validation.

   - Select **Accept AIS Health Check Incidents** to accept AI-Scripts health check incidents from the Service Now end customer.

8. Click **Submit**.

   The end customer is created and displayed on the Organizations page.

Release History Table

Release	Description
15.1R1	Starting Service Now Release 15.1R1, the Accept BIOS Validations check box is provided on the Add Member Dialog Box of a Service Now partner to accept or reject BIOS data from Service Now end customers for validation.

RELATED DOCUMENTATION

Service Now Global Settings Overview | 69

Adding an SNMP Configuration to Service Now | 80

Modifying Organization Parameters

Junos Space Service Now provides the Modify Organization option to modify the parameters of an organization from the Organizations page on Service Now.

You can modify the following parameters of an organization:

- Name of the organization
- Option to submit cases as test cases or real cases
- Username of the organization
- password of the organization
- Site ID of the organization
- JMB filter level

NOTE: A Service Now partner cannot modify the name assigned to end-customer organizations.

To modify the parameters of an organization:

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

   The Organizations page appears.
2. Select the organization whose parameters you want to modify.
3. Click **Modify Organization** from either the **Actions** list or the right-click menu.

The Modify Organization appears.

4. Make changes to the organization parameters.

   For details about organization parameters, see Table 13 on page 123.

5. Click **Submit**.

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

RELATED DOCUMENTATION

Service Now Organizations Overview | 119

Deleting an Organization

Junos Space Service Now provides the Delete option on the Actions list of the Organizations page to delete organizations. You cannot delete an organization when the organization is assigned to the default device group.

NOTE: In a Service Now partner, you cannot delete an organization without first deleting end customers associated with the organization..

To delete an organization:

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

   The Organizations page appears.

2. Select the organization that you want to delete.

3. Click **Delete Organization** from the **Actions** list or the right-click menu.

   The **Delete Organizations** dialog box appears asking you to confirm the deletion.

4. Click **Delete**.

   Service Now deletes the selected organization from the Service Now database and no longer appears on the Organizations page.

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

RELATED DOCUMENTATION

Service Now Organizations Overview | 119

Testing the Connection to JSS

Junos Space Service Now provides the Test Connection option on the Actions list to let you test the connection of every organization with Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode).

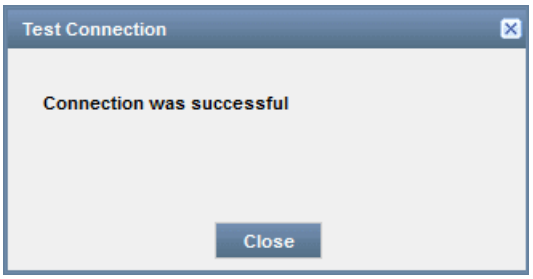
To test an organization's connectivity with JSS:

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

   The Organizations page appears.
2. Select the organization whose connection to JSS you want to test.
3. Click **Check Status** from either the **Actions** list or the right-click menu.

   The **Test Connection** dialog box displays the result of the test connection to JSS or Service Now partner.

Figure 15: Test Connection Dialog Box



   In case of a failure, a description appears stating the reason for the connection failure.
4. Click **Close** to return to the Organizations page.

NOTE: You cannot check the connectivity status when Service Now is operating in the Offline mode.

RELATED DOCUMENTATION

Service Now Organizations Overview | 119

Running an Organization in Test Mode

While configuring an organization, you can enable test mode to submit cases as test cases so as to avoid processing of test cases by Juniper Support Systems (JSS) or Service Now partner. In this mode, the synopsis of the incident that is submitted to JSS is appended with *[Test]*.

To run an organization in test mode:

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

   The Organizations page appears.

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

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

3. Select **Test Cases** from the **Submit Cases as** drop-down list.

4. Click **Submit**.

   Service Now submits incidents with [Test] appended to the incident synopsis for creating cases.

RELATED DOCUMENTATION

Service Now Organizations Overview | 119

Updating Core File Upload Configuration for an End Customer

You can update the core file configuration for a Service Now end customer in Partner Proxy mode. If a Service Now partner is unable to configure an SFTP server for end customers to upload core files, end customers can upload core files to the server used by the Service Now partner. The Service Now partner provides the ID of the case created for an incident to the end customer. The case ID provided by the Service Now partner can be an ID created by the Service Now partner or created by JSS. In either case, the core files are uploaded automatically to the SFTP server once a case is created. For more details, see "Configuring SFTP Server for Uploading Core Files Generated for Events" on page 84.

To change the core file configuration for a connected member:

1. From the Service Now navigation tree, select **Administration** > **Organization**.

   The Organizations page is displayed.

2. Select the organization for which you want to configure the server for uploading core files.

3. Click **Update Core File Upload Configuration** from either the **Actions** list or the right-click menu.

   The Modify Core File Upload Configuration for Connected Member dialog box appears.

4. Fill in the required parameters in the displayed fields, and click **Submit**.

   The Upload Core File Upload configuration is successfully changed.

RELATED DOCUMENTATION

Service Now Organizations Overview | 119

Viewing Messages Assigned to an End Customer | 132

Viewing Messages Assigned to an End Customer

A Service Now partner can view the list of messages that are assigned to an end customer (also known as a connected member). This action is available only when Service Now operates in the Partner Proxy mode and when you select an end customer in the Organizations page.

To view the messages assigned to an end customer:

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

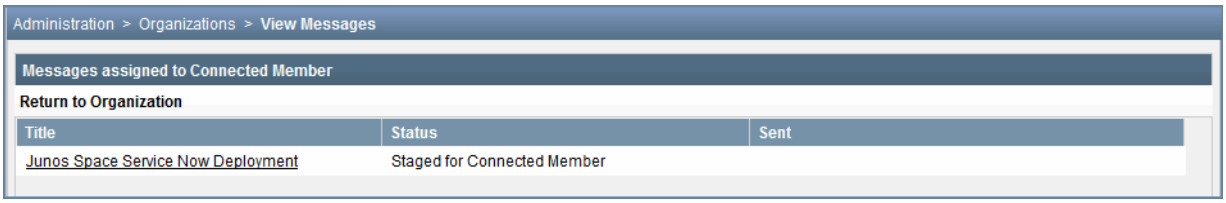
   The Organizations page displays the list of organizations and connected members.

2. Select the end customer organization for which you want to view the assigned messages.

3. Right-click your selection and select **View Messages** from either the **Actions** list or the right-click menu.

   As shown in Figure 16 on page 133, the Messages assigned to Connected Member page displays the list of messages assigned to the selected end customer.

Figure 16: Messages Assigned to Connected Member Page



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 to whom the messages were flagged.

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

RELATED DOCUMENTATION

Assigning a Message to an End Customer

Service Now Messages Overview

8

CHAPTER

Configuring and Managing Device Groups

Service Now Device Groups Overview | **137**

Creating a Device Group | **138**

Modifying a Device Group | **140**

Deleting a Device Group | **142**

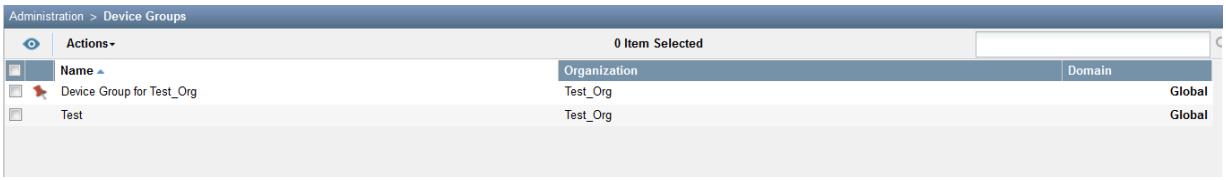
Service Now Device Groups Overview

You can group and manage multiple devices as 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.

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

You can view the device groups configured on Service Now on the Device Groups page (**Administration > Device Groups**) as shown in Figure 17 on page 137.

Figure 17: Core File Upload Configuration Page



Clicking a device group displays the Device Group Detail page where you can view the details of a device group. Table 14 on page 137 lists the parameters on a device group.

Table 14: Device Group Parameters

Parameter	Description
Name	Name of the device group
Organization	Organization to which the device is assigned
Devices	List of devices assigned to the device group
Auto Submit Policies	List of auto submit policies assigned to the device group
Domain	Domain to which the device group is assigned

Associated Actions

You can perform the following actions related to device groups:

- Create a device group and assign devices to it; see “Creating a Device Group” on page 138 for details.
- Modify device groups; see “Modifying a Device Group” on page 140 for details.

- Delete device groups; see “Deleting a Device Group” on page 142 for details.
- Associate address groups; see “Associating Devices with an Address Group from the Device Groups Page” on page 340 for details.
- Set default device group

RELATED DOCUMENTATION

Service Now Devices Overview | 147

Service Now Organizations Overview | 119

Service Now Address Group Overview | 333

Creating a Device Group

You can use device groups to group devices within an organization. Only users with Service Now administrator privileges can create device groups and add devices to them. A device added newly to Service Now is assigned to the default device group.

Device Group in Direct or End Customer mode:

- When a new organization is created, Service Now automatically creates a device group and associates it with the organization.
- You can edit and delete the default device groups that Service Now creates for organizations.

Device Group in Partner Proxy Mode:

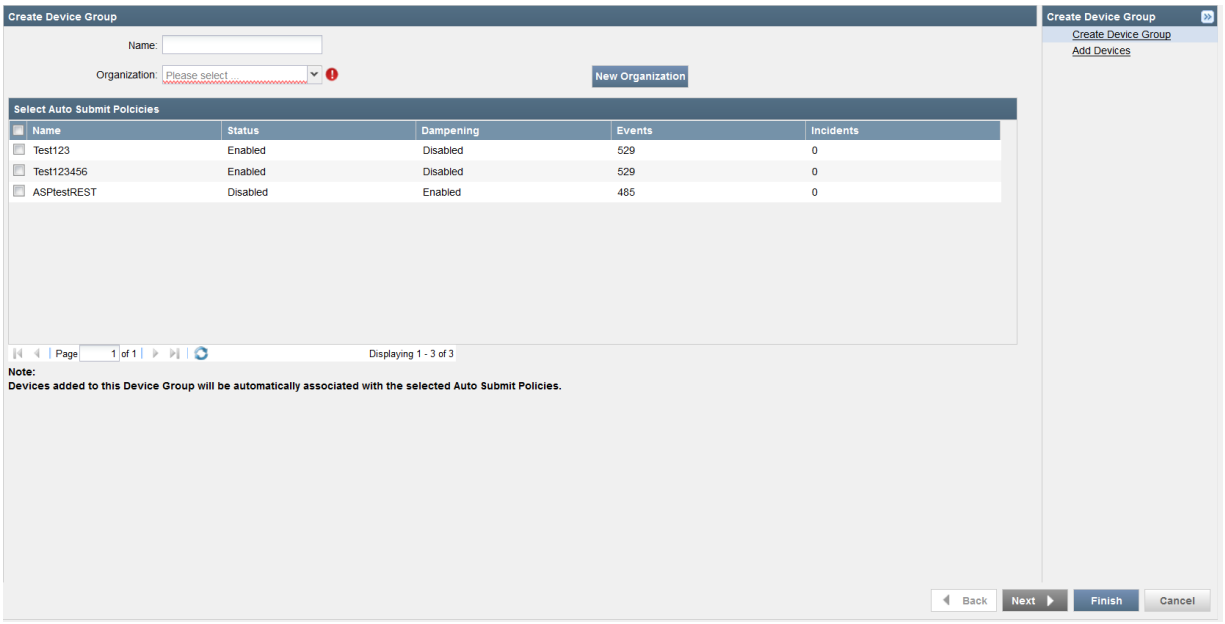
- When a new organization is created, Service Now automatically creates a default device group and associates it with the organization.
- Service Now creates a default device group the organization created by an end customer.
- Devices added by end customers are automatically added to the default device group.
- Administrators can edit but not delete the default device group for end customers.

To create a device group:

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

   The Create Device Group page appears.

Figure 18: Create Device Group Page



2. Enter a name for the device group in 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 (-). The maximum number of characters allowed is 64.
3. In the **Organizations** list, select an organization to associate with this device group.

   If you want to associate the device group with a new organization, click **New Organization** and configure the new organization. See "Adding an Organization to Service Now" on page 122 for details.
4. (Optional) In the Select Auto Submit Policies section, select one or more auto submit policies that you want to associate with the device group.
5. Click **Next** to add devices to the device group or click **Finish** to create the device group.

   When you click Next, the Add Devices page appears.
6. Select the devices that you want to add to this device group from the **Select Device to add them to the Device Group** section.
7. Click **Finish**.

   Service Now adds the selected devices to the device group.

To verify if the devices are added to the device group, double-click the device group on the Device Groups page. The Device Group Detail page lists the devices and auto submit policies that are assigned to the device group.

RELATED DOCUMENTATION

Service Now Devices Overview | 147

Service Now Auto Submit Policy Overview | 237

Modifying a Device Group

Service Now provides the Modify Device Group option in the Actions list to modify configured device groups. You can modify the following parameters of a device group:

- Name of the device group
- Organization associated with the device group
- Default status of the device group
- Auto submit policies associated with the device group
- Devices included in the device group

To modify a device group:

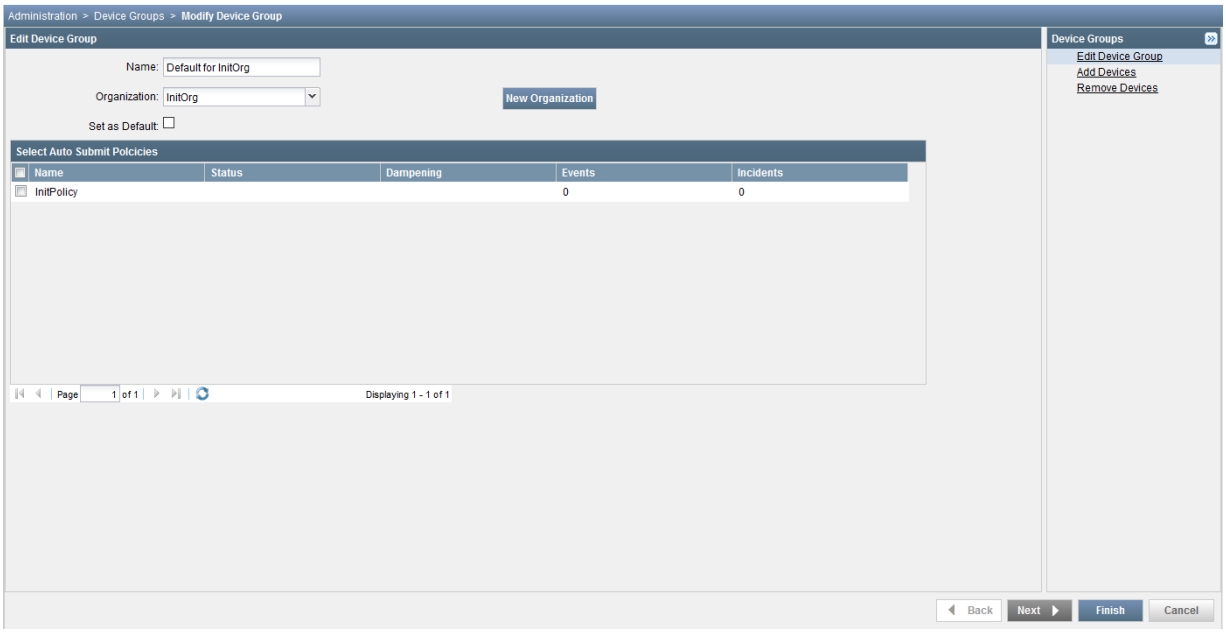
1. From the Service Now navigation tree, select **Administration** > **Device Groups**.

   The 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** list or the right-click menu.

   The Edit Device Group page appears and displays the configuration of the selected device group.

Figure 19: Associate Case ID Dialog Box



3. (Optional) In the **Name** text field, modify the name of the device group.
4. (Optional) In the **Organization** drop-down list, modify the organization associated with the device group.

   If required, click the **New Organization** button to create a new organization and associate it with the device group. For information about creating a new organization, see "Adding an Organization to Service Now" on page 122.
5. (Optional) Select the **Set as Default** check box to set the device group as the default device group in Service Now.

   For Service Now running in Partner Proxy mode, you can set any device group as the default while modifying the device group. . However, if the user does not select the **Set as Default** check box, an error message appears as follows—**Please set other device group as the default device group before unselecting this device group as the default**.
6. (Optional) Add or remove one or more auto submit policies assigned to the device group by selecting or clearing the check boxes next to the auto submit policies.

   TIP: Use the **Device Groups** navigation drawer on the right-hand side of the page to add or delete devices from the selected device group.
7. Click **Next** to add devices to the device group or click **Finish** to submit the changes.

   If you click Next, Service Now displays the Add Devices page.
8. (Optional) Select one or more devices to add to the device group.

9. Click **Next** to remove devices from the device group or click **Finish** to submit the changes.

   If you click Next, the Remove Devices page appears.

10. (Optional) Select one or more devices to be removed from the device group.

11. Click **Finish**.

    Service Now modifies the device group and displays the Device Group page.

12. You can verify the changes by double-clicking the modified device group.

    The Device Group Detail page appears displaying the devices and auto submit policies assigned to the device group..

RELATED DOCUMENTATION

Service Now Device Groups Overview | 137

Service Now Devices Overview | 147

Deleting a Device Group

Junos Space Service Now provides the Delete option in the Actions list on the Device Groups page to delete device groups. You cannot delete a default device group.

To delete a device group:

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

   The 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** list or the right-click menu.

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

3. Click **Delete**.

   Service Now deletes the selected device group is deleted from the Service Now database and the device group no longer appears on the Device Groups page.

RELATED DOCUMENTATION

Service Now Device Groups Overview | 137

Creating a Device Group | 138

9

CHAPTER

Managing Service Now Devices

Service Now Devices Overview | **147**

Adding Devices to Junos Space Service Now | **155**

Installing an Event Profile on a Device by Using Service Now | **156**

Manually Installing AI-Scripts on Devices | **160**

Uninstalling an Event Profile from a Device | **165**

Configuring AI-Scripts Parameters by Using Junos Space Service Now | **167**

Deleting a Device from Junos Space Service Now | **170**

Associating Devices with a Device Group | **171**

Assigning an Auto Submit Policy to a Device | **172**

Generating an On-Demand Incident | **174**

Generating an On-Demand Device Snapshot | **180**

Generating an RMA Incident for a Device | **182**

Verifying the Connection Between a Device and the SFTP Server | **186**

Collecting RSI and System Log Files | **187**

Configuring BIOS Validation for Verifying BIOS Integrity of a Device | **191**

Exporting Device Data in CSV and Excel Formats | **193**

Exporting Inventory Information in CSV Format | **195**

Viewing Incidents Created for a Device | **196**

Viewing Exposure for a Device | **196**

Moving a Device to Maintenance Mode | **198**

Service Now Devices Overview

For Junos Space Service Now to monitor and detect events on devices, you must discover the devices by using the Junos Space Network Management Platform, add the devices to Service Now, and then install AI-Scripts on the devices.

You can view only those devices discovered by the Junos Space Platform for which you have permission (based on the role-based access control [RBAC] policy). When you add a device to Service Now, you receive information JMBs (iJMBs) and event JMBs (eJMBs) that help you monitor and resolve issues on the device. You can view devices added to Service Now on the Service Now Devices page (**Administration > Service Now Devices**).

You can group multiple devices into a single device group so that you can manage these devices as a single entity; for example, you can install or uninstall AI-Scripts on all the devices in a device group in a single operation.

You can view Service Now devices on the Service Now devices page. Double-click a device to view its details. Details about a device are displayed under the following five tabs—Details, Address Details, Contract Details, Device Analysis, and Advanced Params Settings..

- Details—Provides general details such as the hostname, IP Address, and serial number of the device
- Address Details—Provides the ship-to-address and location where the device is present
- Contract Details—Provides service contract details of the device

> **NOTE:** Service Now populates the details of the start and end dates of contract and end-of-life (EOL) information of the device components on the View Physical Inventory page of the Junos Space Network Management Platform GUI. For details about accessing the View Physical Inventory page, see Viewing Physical Inventory.

  Starting in Service Now Release 16.1R1, a Service Now partner does not send the service contract information for end customer devices to end customers. However, the contract information for end-customer devices can be viewed on the Service Now partner.

- Device Analysis—Provides details such as the Routing Engine, and time and status of the data collected from the device for validating the BIOS integrity of the device
- Advanced Param Settings—Displays AI-Scripts-related configuration for the device

Table 15 on page 148 describes the attributes of Service Now devices displayed under the four tabs.

Table 15: Service Now Devices Field Descriptions

Field Name	Description
Details tab	
Organization	Name of the organization to which the device is assigned.
Connected Member	Name of the connected member.
Device Group	Name of the device group to which the device belongs.
HostName	Unique name by which the device is known on a network.
IP Address	IP address of the device.
Serial Number	Serial number of the device.
Product	Type of the device; for example, MX960 and EX4200.
Platform	Model of the device.
OS Version	Version of the Junos OS that is running on the device.
State	By default, this field is hidden. This field is displayed only for end-customer devices in a Service Now application operating in the Partner Proxy mode. The values for this field are Added and Removed.
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.
Routing Engine	Type of Routing Engine present on the device; the values are: • Single Routing Engine • Dual Routing Engines
Event Profile Installation Status	Installation status of an event profile on the device; the values are: • Success • Failed • Master RE Failed • Backup RE Failed • Successfully installed in Master RE; Backup RE is inactive

Table 15: Service Now Devices Field Descriptions *(continued)*

Field Name	Description
Policy	Auto submit policies associated with the device for submitting incidents to a Service Now partner (for Service Now operating in End Customer mode) or Juniper Support Systems (JSS); when a device is associated with more than one auto submit policy, each policy is separated by a comma.
RSI File Collection	Configuration for collecting RSI from the device.
BIOS File Collection	Configuration for collecting BIOS files from the device.
Log File Collection	Configuration for collecting system log files from the device.
Connection Status	Status of connection between the device and Service Now.
Maintenance Mode	Specifies whether the device is currently in maintenance mode or not. Possible values are: • ON: The device is in maintenance mode. • OFF: The device is not in maintenance mode.
Alerts	Status of iJMB received from the device.
Support Contract Information	Table to display information about the support contract for the device. The following fields are included in the table: contract number, status, SKU, SKU type, as well as start and end dates of the contract. To receive on-demand updates about your Service Now contract, click the **Refresh** button on the Device Details page.
Address Details tab	
Ship-to Address	Address to which the device or device parts should be shipped.
Location	Location the device is installed.
Contract Details tab	
Contract #	Service contract number of the device.
Status	Status of the device service contract.
SKU	Stock-keeping unit of the device.

Table 15: Service Now Devices Field Descriptions *(continued)*

Field Name	Description
SKU Type	Type of SKU of the device.
Start Date	Start date of the device service contract.
End Date	End date of the device service contract.
Serial Number	Serial number of the device.
Device Analysis tab	
Entity	Routing Engine from which data was collected for BIOS validation.
Type	Type of device analysis.
Last Collected	Date and time when the data was last collected for BIOS validation.
Status	Status of BIOS validation: • Pending Submission—Service Now has received data for BIOS validation from the device; the data is yet to be submitted to Juniper Support Systems (JSS) or Service Now partner (in case of end customer mode). • Pending Case Creation—BIOS validation data of the device is received by JSS; JSS is yet to create a case for the received data. • Case Created—JSS has created a case for the BIOS validation data received for the device. **NOTE:** This status is not applicable if Service Now is operating in the End Customer mode. • Case Creation Failed—JSS failed to create a case for the BIOS validation data received for the device. **NOTE:** This status is not applicable if Service Now is operating in the End Customer mode. • Submission Failed—Service Now is unable to submit the BIOS validation data of the device to JSS or Service Now partner • Validation Success—The validation of BIOS data of the device by JSS or Service Now partner was successful. • Out for Extended Review—The BIOS validation encountered issues and the BIOS data is sent to the device team for further review.
Advanced Params Settings	

Table 15: Service Now Devices Field Descriptions *(continued)*

Field Name	Description
JMB cleanup age	Number of days after which JMBs are deleted from the device.
Device snapshot collection day of the week	Day of the week when device snapshot should be collected from the device.
Device snapshot collection time of the day	Time of the day when device snapshots should be collected from the device.
Collect logs from all nodes	Indicates if system log files can be collected from all the Service Now devices.
Maximum events to be simultaneously processed on-box	Number of events that AI-Scripts can process when multiple events occur on the device at the same time.
Threshold % of disk usage for warning messages	Percentage of disk used beyond which AI-Scripts should log a warning message indicating that the disk usage has reached the specified threshold.
Threshold % of disk usage for data dampening	Percentage of disk used after which AI-Scripts should not generate JMBs when one or more events occur on the device.

The icon, when displayed on the left-side of a row on the Service Now Devices page, indicates one of the following scenarios:

- There is a mismatch between the versions of AI-Scripts installed on the device and AI-Scripts bundle present on Service Now.

  This icon is also displayed when Service Now does not have an AI-Scripts bundle uploaded, but the device has AI-Scripts installed on it.

  If you place the cursor on the icon, the tool tip displays the following message:

  ```
  There is a mismatch of the AI-Scripts installed on routing engine, on device.
  ```

  For example:

  ```
  There is a mismatch of AI-Scripts installed on 'fpc0' of device ex-4200-sn1.
  ```

  For a device with dual Routing Engines, *routing engine* indicates the Routing Engine on which the version of AI-Scripts installed is different from the AI-Scripts bundle present on Service Now. If the version of AI-Scripts installed on both the Routing Engines is different from the AI-Scripts bundle present on Service Now, the following message is displayed:

```
There is a mismatch of the AI-Scripts installed on routing engine 1, routing
engine 2, on device.
```

For example:

```
There is a mismatch of AI-Scripts installed on 're0', 're1' of device mx-104-sn.
```

There can be a mismatch between the versions of AI-Scripts installed on a device and Service Now for the following reasons:

- Service Now is unaware of the AI-Scripts version installed on a device—for example, when you add a device to Service Now that already has AI-Scripts installed on it.
- After installing AI-Scripts on a device by using Service Now, you have manually deleted AI-Scripts from the device.

- One or more JMB files, attachments, and log files are not deleted from a device after these files are copied from the device to Service Now.

  If you place the cursor on the icon, a tool tip displays the following message:

  ```
  one or more files (JMB/Attachments/Logs) could not be deleted from the device.
  ```

  These files contain the **_ais_** string in their names and must be deleted manually from the **/var/tmp** directory of the device.

- The device does not have a service contract.

  NOTE: Starting in Service Now Release 16.1R1, you see a tool tip on the Service Now Devices page when the device does not have a service contract. In addition to the service contract for the main chassis, Service Now also displays service contracts available for all parts of a device on the Device Details page.

Associated Actions

You can perform the following actions related to Service Now devices:

- View details of a device.
- Add devices from the Junos Space Platform to Service Now; see "Adding Devices to Junos Space Service Now" on page 155 for details.
- Install event profiles on the devices; see "Installing an Event Profile on a Device by Using Service Now" on page 156 for details.
- Uninstall event profiles from the devices; see "Uninstalling an Event Profile from a Device" on page 165 for details.
- Configure BIOS validation; see "Configuring BIOS Validation for Verifying BIOS Integrity of a Device" on page 191 for details.
- Configure product health data collection (PHDC); see "Configuring Product Health Data Collection on a Device" on page 300 for details.
- Export device data in CSV and Excel formats; see "Exporting Device Data in CSV and Excel Formats" on page 193 for details.
- Delete devices from Service Now; see "Deleting a Device from Junos Space Service Now" on page 170 for details.
- Associate devices with a device group; see "Associating Devices with a Device Group" on page 171 for details.
- Associate auto submit policies with devices; see "Assigning an Auto Submit Policy to a Device" on page 172 for details.
- Export inventory information in CSV format; see "Exporting Inventory Information in CSV Format" on page 195 for details.
- View the devices that are susceptible to known issues; see "Viewing Exposure for a Device" on page 196 for details.
- Generate on-demand incidents; see "Generating an On-Demand Incident" on page 174 for details.
- Generate on-demand device snapshot; see "Generating an On-Demand Device Snapshot" on page 180
- Request RMA incidents; see "Generating an RMA Incident for a Device" on page 182 for details.
- Associate devices with an address group; see "Associating Devices with an Address Group from the Service Now Devices Page" on page 341 for details.
- Verify the connection between the devices and the SFTP server; see "Verifying the Connection Between a Device and the SFTP Server" on page 186 for details.
- View incidents created for a device; see "Viewing Incidents Created for a Device" on page 196 for details.
- Configure RSI and log file collections; see "Collecting RSI and System Log Files" on page 187 for details.

- Assign a device to another domain; see "Assigning a Service Now Object to Another Domain" on page 56 for details.
- Move a device to maintenance mode; see "Moving a Device to Maintenance Mode" on page 198 for details.

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16.1R1, a Service Now partner does not send the service contract information for end customer devices to end customers. However, the contract information for end-customer devices can be viewed on the Service Now partner.
16.1R1	Starting in Service Now Release 16.1R1, you see a tool tip on the Service Now Devices page when the device does not have a service contract. In addition to the service contract for the main chassis, Service Now also displays service contracts available for all parts of a device on the Device Details page.

RELATED DOCUMENTATION

Service Now Device Groups Overview | **137**

Service Now Event Profiles Overview | **203**

Service Now Auto Submit Policy Overview | **237**

Service Now BIOS Validation Overview

Product Health Data Collection Configuration Overview | **297**

Service Now Incidents Overview

Adding Devices to Junos Space Service Now

Junos Space Service Now adds devices discovered by Junos Space Network Management Platform automatically if the devices are discovered after Service Now is installed on Junos Space Platform. Howevere, if you discover devices after Service Now is installed, you have manually add the discovered devices to Service Now.

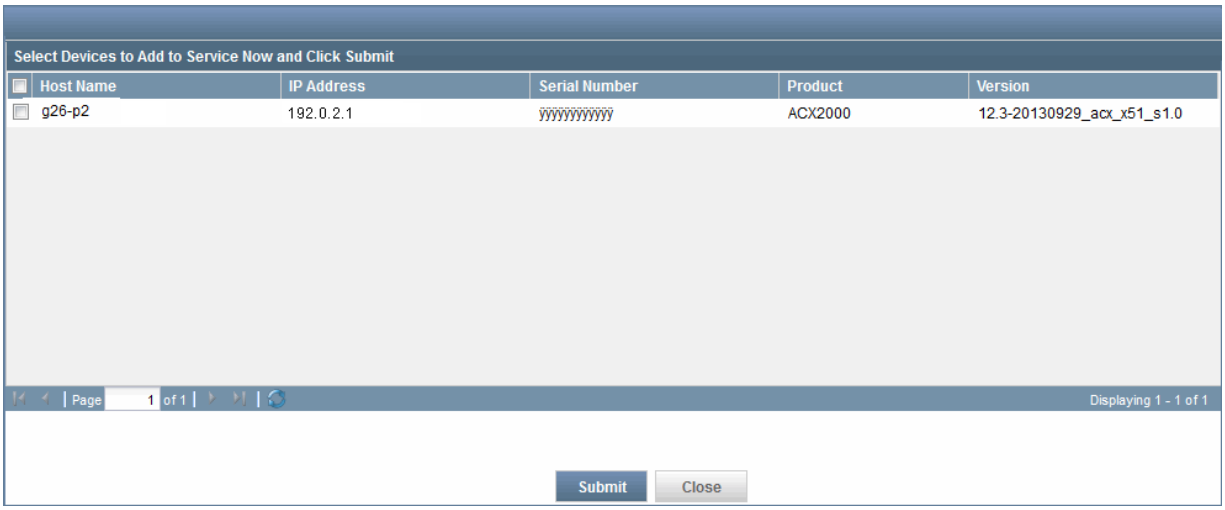
Service Now provides the Add Devices option in the Service Now Devices task of the Service Now navigation tree to add devices.

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

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

   The Select Devices to Add to Service Now and Click Submit page displays the devices that are discovered by Junos Space Platform, but not added to Service Now.

Figure 20: Select Devices to Add to Service Now and Click Submit Page



2. Select the devices that you want to add.

3. Click **Submit**.

   The Service Now Devices page appears and lists the devices added to Service Now..

RELATED DOCUMENTATION

Installing an Event Profile on a Device by Using Service Now | 156

Assigning an Auto Submit Policy to a Device | 172
Juniper Networks Devices Supported by Service Now and Service Insight | 46

Installing an Event Profile on a Device by Using Service Now

An event profile defines a set of event policies selected from an AI-Scripts bundle to generate Juniper Message Bundles (JMBs) for informing users about an event when the event occurs on a device.. When you install an event profile on managed devices, the event policies detect the events that occur on devices and automatically provide the information needed to troubleshoot the events.

Service Now uses the 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 devices with dual Routing Engines, Service Now installs the event profile on both primary and backup Routing Engines.

NOTE:

- A Service Now partner cannot install event profiles on a Service Now end-customer's devices.
- For information about behavior of AI-Scripts when installed on specific product families, see https://kb.juniper.net/InfoCenter/index?page=content&id=KB29188.

The icon appears on the left side of a device row on the Service Now Devices page if the versions of the AI-Scripts installed on the device and Service Now are different. For a device with dual Routing Engine, the icon also indicates that the version of the AI-Scripts installed on the primary and backup Routing Engines are different. If you place the cursor on the icon, the tool tip displays a message similar to the following:

There is a mismatch of the AI-Scripts installed on *routing engine* on *device*.

To install an event profile on devices:

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

   The Service Now Devices page appears.

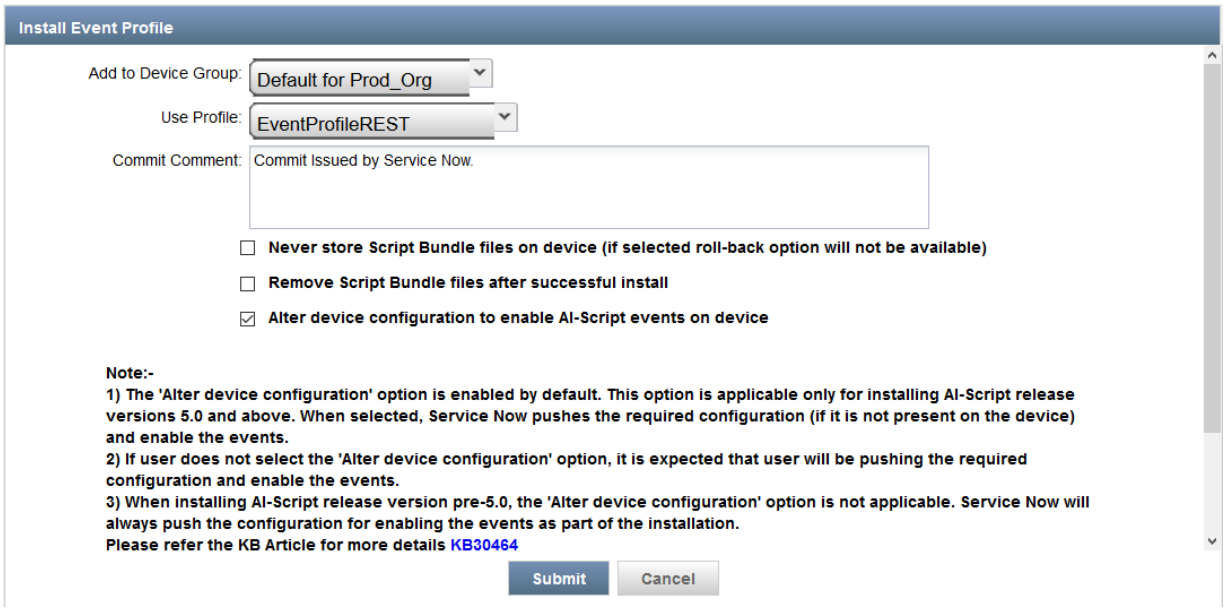
2. Select the device on which you want to install the event profile.

The Install Event Profile action is active even if the devices are not associated with an organization or Device Group.

3. From the Actions list or right-click menu, select **Device Operations > Install Event Profile**.

   The Install Event Profile page appears as shown in Figure 21 on page 157.

Figure 21: Install Event Profile Page



4. Select a device group from the **Add to Device Group** drop-down list to add the device to the device group.

5. Select an event profile from the **Use Profile** drop-down list to assign to the device.

6. (Optional) Enter your comments for installing the event profile in the **Commit Comment** text box.

   The maximum number of characters allowed is 225. Service Now adds a default comment as **Commit Issued by Service Now for enabling AI-Scripts**.

> **NOTE:** This option is not available if the Alter device configuration to enable AI-Script events on device check box is not selected.
>
> When a Service Now device is deleted from Service Now, the commit comment present in the Advanced Settings page is used while committing AI-Scripts configuration on a device.
>
> You can view the commit comment on a device by executing the **show system commit** command.

7. (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.

   > **NOTE:** This option is not available during the installation of event profiles on the QFX3000-M, QFX3000-G and EX Series devices with dual Routing Engines.

8. (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.

   > **NOTE:** This option is not available during the installation of event profiles on QFX3000-M, QFX3000-G, and EX Series devices with dual Routing Engines.

9. (Optional) if you do not want the device configuration to be modified while committing the event profile on the device, clear the **Alter device configuration to enable AI-Script events on device** check box.

   By default, this option is selected.

NOTE:

- If you clear the **Alter device configuration to enable AI-Script events on device** check box and the static AI-Scripts configuration is not present on the device, Service Now only installs the AI-Scripts bundle on the device. The static AI-Scripts configuration must be committed on the device manually and the **/var/db/scripts/op/ais-param-set.slax** file executed for AI-Scripts to generate JMBs.
- When you install or upgrade AI scripts releases earlier than Release 5.0 on a device using Service Now Release 15.1 or later, the static AI-Scripts configuration must be pushed manually to the device for each installation and upgrade irrespective of whether the Alter device configuration to enable AI-Script events on device check box is selected or cleared.

10. (Optional) If you want to schedule a time for installing the event profile, 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.

11. Click **Submit**.

12. (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.

13. Click **Finish**.

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

14. Do one of the following: Click one of the following links based on the required results.

- Apply the event profile to devices manually.

  To apply the event profile to devices manually:

  a. Click the **Apply this Event Profile to Devices manually** link.

  b. Click the devices on which you want to apply the event profile.

  c. 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. The Jobs page displays the status of the job. Double-click the job to view information about each step of the installation.

  d. Click **OK** to return to the Event Profiles page.

- Return to the Event Profiles page

  Click **Return to the Event Profiles Page** to return to the Event Profiles page.

RELATED DOCUMENTATION

Service Now Event Profiles Overview | 203

AI-Scripts Overview | 21

Manually Installing AI-Scripts on Devices | 160

Adding a Script Bundle to Junos Space Service Now | 226

Viewing Exposure for a Device | 196

Manually Installing AI-Scripts on Devices

AI-Scripts Releases prior to 5.0R2.0 can be installed on Junos OS devices manually by 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 Network Management Platform.

> **NOTE:** We recommend that you install AI-Scripts on devices during a maintenance window.

To install AI-Scripts Release 4.XRX or earlier manually on a device:

1. Copy the AI-Scripts install package (example: **jais-4.0R1.0-signed.tgz**) to the Junos OS device using SCP or FTP.

2. Install the AI-Scripts bundle install package in CLI mode by using one of the following commands:

   - **request system scripts add <*pathname*>**, where <*pathname*> is the path to the AI-Scripts bundle copied on the device.
   - **request system software add <*package-name*> <*node*>**, where <*node*> is the Routing Engine—re0 or re1 and <*package-name*> is the name of the AI-Scripts bundle copied on the device.

NOTE:

- The **request system software add *<pathname>* *<node>*** command when executed on a master Routing Engine installs AI-Scripts on all backup Routing Engines of a device.
- We recommend that the AI-Scripts installation package be placed in the **/var/tmp/** directory as some platforms require the package to be stored in the **/var/tmp/** directory.
- 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.

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

3. Verify that AI-Scripts is installed on all Routing Engines of the device by using the **show version** command.

   AI-Scripts is installed on the device if AI-Scripts *[version]* is displayed in the output of the **show version** command.

4. 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/

   NOTE: For QFabric devices, use the following command:

   set fabric administration ais enable

5. Commit the static AI-Scripts configuration.

To install AI-Scripts 5.0 (5.0R2, 5.0R3, and 5.0R4) and later releases manually on a device:

> **BEST PRACTICE:** We recommend you to use Service Now to install AI-Scripts Release 5.0R2.0 and later. For information about installing AI-Scripts Release 5.0R2.0 and later on a device by using Service Now, see "Installing an Event Profile on a Device by Using Service Now" on page 156.

> **NOTE:**
> - AI-Scripts Release 5.0R2.0 or later cannot be installed on QFabric devices.
> - You cannot install AI-Scripts Release 6.0R1 and later on a device manually. Service Now displays a warning message on the Service Now GUI when AI-Scripts Release 6.0R1 and later is manually installed on a device.

1. Copy the AI-Scripts install package (example: jais-5.0R2.0-signed.tgz) to the Junos OS device using SCP or FTP.

2. Install the AI-Scripts bundle install package in CLI mode by using one of the following commands:
   - **request system scripts add <*pathname*>**, where <*pathname*> is the path to the AI-Scripts bundle copied on the device.
   - **request system software add <*pathname*> <*node*>, where<*node*> is the Routing Engine—re0 or re1 and <*package-name*> is the name of the AI-Scripts bundle copied on the device.**

     > **NOTE:**
     > - The **request system software add <*pathname*> <*node*>** command when executed on a master Routing Engine installs AI-Scripts on all backup Routing Engines of a device.
     > - We recommend that the AI-Scripts installation package be placed in the **/var/tmp/** directory as some platforms require the package to be stored in the **/var/tmp/** directory.
     > - 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.

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

3. Verify that AI-Scripts is installed on all Routing Engines of the device by using the **show version** command.

4. For AI-Scripts Release 5.0R1 and later, enter the configuration mode on the device and add the static AI-Scripts configuration as follows:

```
set groups juniper-ais system scripts op file ais_change_perm.slax
set groups juniper-ais system scripts op file ais_core_perm.slax
set groups juniper-ais system scripts op file on-demand.slax
set groups juniper-ais system scripts op file remove-jais.slax
set groups juniper-ais system scripts op file ais_arc.slax
set groups juniper-ais system scripts op file ais-attach-file.slax
set groups juniper-ais system scripts op file stop-ais-now.slax
set groups juniper-ais system scripts op file ais_signalSN.slax
set groups juniper-ais system scripts op file ais_core_chm.slax
set groups juniper-ais system scripts op file ais_all_chm.slax
set groups juniper-ais system scripts op file att_signalSN.slax
set groups juniper-ais system scripts op file ais-rsi-chk.slax
set groups juniper-ais system scripts op file ais-param-set.slax
set groups juniper-ais system scripts op file ais-sleep.slax
set groups juniper-ais system scripts op file ais-error.slax
set groups juniper-ais system scripts op file ais-health-report.slax
set groups juniper-ais system scripts op file ais_xfer_jmb.slax
set groups juniper-ais system scripts op file ais_policy_create.slax
set groups juniper-ais event-options event-script max-datasize 128m
set groups juniper-ais event-options event-script file intelligence-event-main.slax
set groups juniper-ais event-options event-script file bios.slax
set groups juniper-ais event-options event-script file phdc.slax
set groups juniper-ais event-options event-script file Master-event-struct.slax
set groups juniper-ais event-options event-script file Master-event-unstruct.slax
set groups juniper-ais event-options event-script file Master-policy-events.slax
set groups juniper-ais event-options event-script file User-event-struct.slax
set groups juniper-ais event-options event-script file User-event-unstruct.slax
set groups juniper-ais event-options event-script file User-policy-events.slax
set groups juniper-ais event-options event-script file jais-scripts-add.slax
set groups juniper-ais event-options destinations juniper-aim archive-sites
/var/tmp
set apply-groups juniper-ais
```

5. Commit the static AI-Scripts configuration.

> **BEST PRACTICE:** We recommend that you commit the AI-Scripts configuration during a maintenance window.
>
> On a multichassis system, use the **commit synchronize** command so that the AI-Scripts configuration is committed on all Routing Engines.

6. Do one of the following to activate the event profile

   - If using the **AISevent_info_default.xml** file to define the event profile, edit the **AISevent_info_default.xml** file to include the events that you want to monitor on the device.

     The **AISevent_info_default.xml** file is present at the **/var/db/scripts/commit** location and includes all the event definitions that are available for a release. The default event profile automatically excludes events that are not valid for a device.

     Use the **op ais-param-set event-file default** command to activate the event profile.

     > **BEST PRACTICE:** On a multichassis system, execute the command on the master Routing Engine.

   - If using the **AISBundle_info.xml** file to define event profile, verify that the **AISBundle_info.xml** file is present in the **/var/db/scripts/commit/** location.

     The file contains the definitions for the events to be monitored on the device and is stored on the device by Service Now while installing AI-Scripts.

     Use the **op ais-param-set event-file /var/db/scripts/commit/AISBundle_info.xml** command to activate the event profile.

The event profile is installed and configured on the device.

RELATED DOCUMENTATION

Adding a Script Bundle to Junos Space Service Now | 226

Uninstalling an Event Profile from a Device

Junos Space Service Now provides the Uninstall Event Profiles from managed devices option in the Actions list of the Service Now Devices page to uninstall event profiles. . Service Now uses Device Management Interface (DMI) to install and uninstall event profiles from devices. DMI is an extension to the NETCONF network management protocol.

> **NOTE:** A Service Now partner cannot uninstall event profiles from a Service Now end-customer's devices.

To uninstall event profiles from a managed device:

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

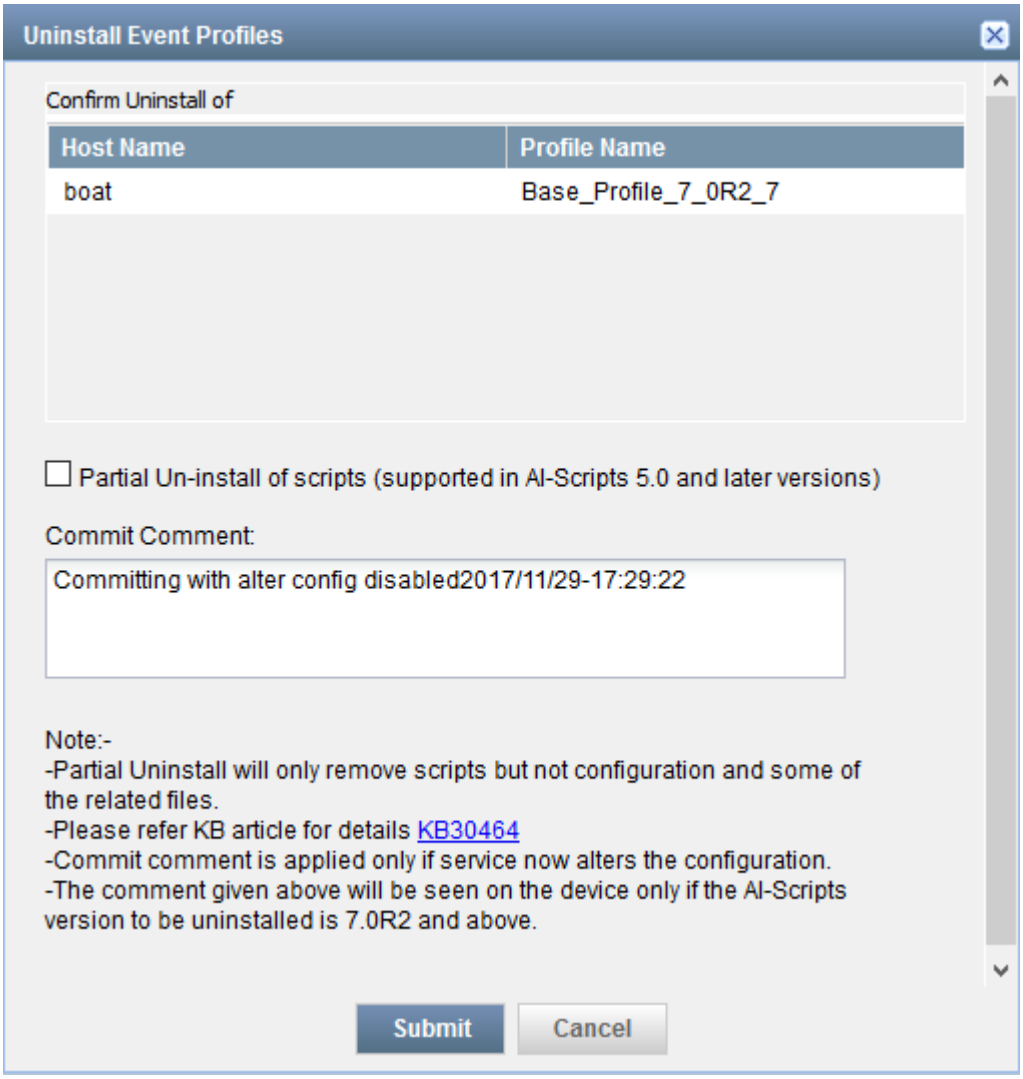
   The Service Now Devices page appears.

2. Select the device from which you want to uninstall the event profile.

3. From the Actions list or right-click menu, select **Device Operations > Uninstall Event Profile**.

   The Uninstall Event Profile dialog box appears as shown in Figure 22 on page 166.

Figure 22: Uninstall Event Profiles Dialog Box



4. (Optional) Enter your comments for uninstalling the event profile in the **Commit Comment** text box.

   The maximum number of characters allowed for a comment is 225. Service Now enters a default comment as **Commit Issued by Service Now for disabling AI-Scripts**.

> **NOTE:** This option is available only when AI-Scripts Release 7.0R2 is installed on Service Now Release 17.2R1.
>
> When you delete a device from Service Now, AI-Scripts configuration is first deleted from the device. While deleting the AI-Scripts configuration, the commit comment provided on the Advanced Settings page is used as the comment for committing the AI-Scripts configuration on the device.
>
> You can view the commit comment on a device by executing the **show system commit** command.

5. Select the **Partial Un-install of scripts(Supported in AI-Script 5.0 and above versions)** check box to avoid the AI-Scripts configuration from being modified when uninstalling the event profile from the device.

   > **NOTE:** If you uninstall AI-Scripts Release 5.0 or later with the **Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)** option cleared, ensure that the AI-Scripts configuration is deleted manually by executing the **/var/db/scripts/remove-jais.slax** script to avoid errors while committing the next AI-Scripts configuration (during installation or upgrade of Junos OS on the device).

6. Click **Submit**. A job to uninstall the event profile is initiated.

   Click the *job ID* link to view the status of the job.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Configuring AI-Scripts Parameters by Using Junos Space Service Now

AI-Scripts parameters such as duration after which a JMB should be deleted from the device, day and time for collecting intelligence JMBs (or device snapshots), and so on are configured by using the

ais-param-set.slax file that is present in the AI-Scripts bundle. Starting Junos Space Service Now Release 17.2R1, Service Now provides the Advanced Parameters Settings option in the Actions list to configure the AI-Scripts parameters from the Junos Space Service Now GUI.

> **NOTE:** We recommend that you configure AI-Scripts parameters on a device by using Service Now after you consult with Juniper Networks support team.

To configure AI-Scripts parameters from the Service Now GUI:

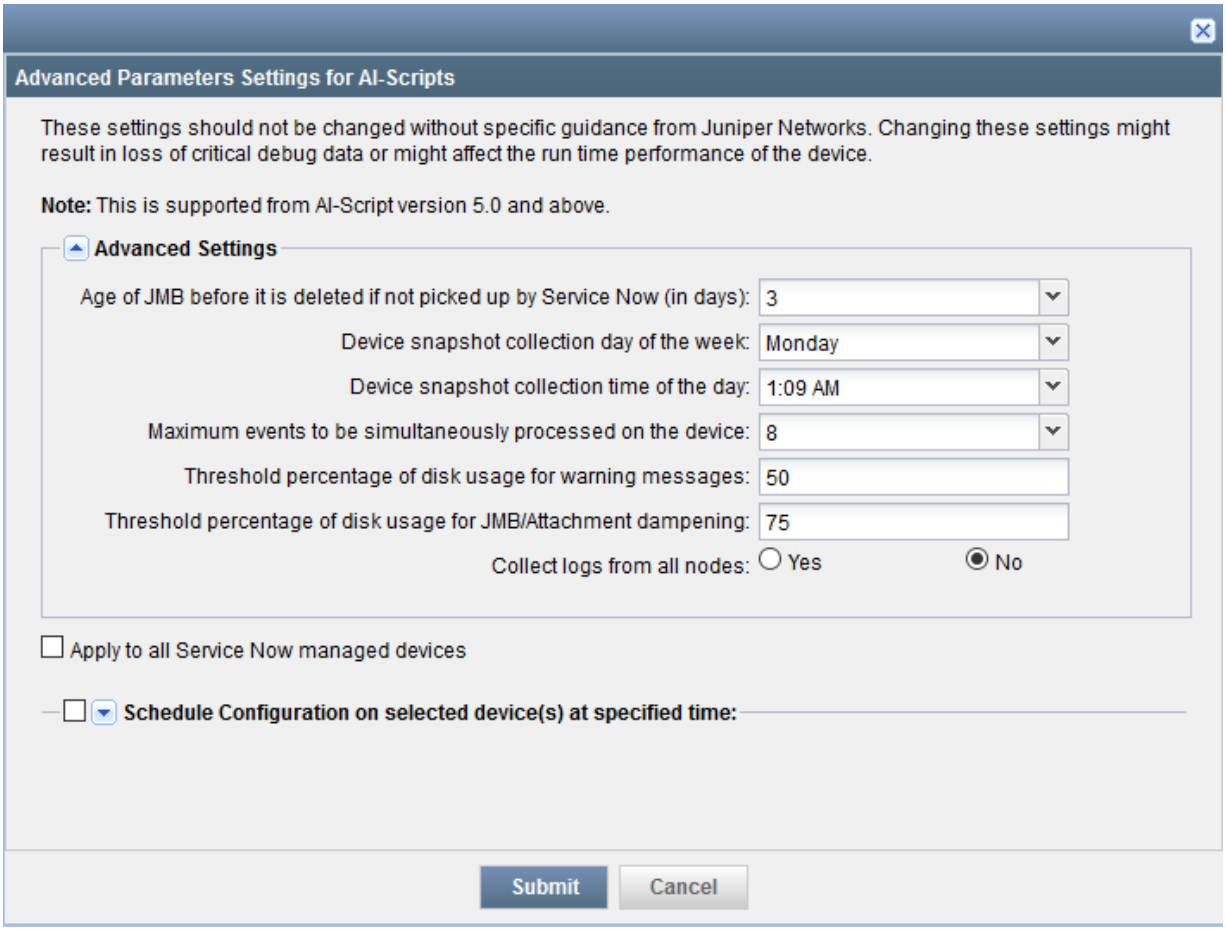
1. From the Navigation tree, navigate to **Administration > Service Now Devices**.

   The Advanced Parameters Settings dialog box appears.

2. Select one or more devices on which you want to configure the AI-Scripts parameters and select **Device Operations > Advanced Parameters Settings** from the Actions list or the right-click menu.

   The Advanced Parameter Settings for AI-Script dialog box appears as shown in Figure 23 on page 169.

Figure 23: Advanced Parameters Settings for AI-Scripts



3. If the AI-Scripts parameters are not visible, click the down arrow next to Advanced Settings to view AI-Scripts parameters.

   The AI-Scripts parameters are displayed.

4. Enter values for the AI-Scripts parameters as follows:

   - **Age of before it is deleted if not picked up by Service Now (in days):** Select the number of days after which AI-Scripts should delete JMBs from the device.
   - **Device snapshot collection day of the week:** Select the day of the week when AI-Scripts should execute scripts for collecting device snapshot from the device.
   - **Device snapshot collection time of the day:** Select a time of the day from when AI-Scripts should execute scripts for collecting device snapshot from the device.

     This list provides values at an interval of 15 minutes. You can also enter any value other than the listed values; for example, 1:10 AM, 2:20 AM, 4:05 PM, and so on.

- **Maximum events to be simultaneously processed on the device:** Select the number of events that AI-Scripts can process when multiple events occur on the device at the same time.

  You can configure values from 1 to 15.

- **Threshold percentage of disk usage for warning messages:** Enter the disk usage limit, in terms of percentage, beyond which AI-Scripts should log a warning message to indicate that the disk usage has reached the specified threshold.

- **Threshold percentage of disk usage for JMB/Attachment dampening:** Enter the disk usage limit, in terms of percentage, after which AI-Scripts should not generate JMBs when one or more events occur on the device.

- **Collect logs from all nodes:** Select **Yes** to allow AI-Scripts to collect system log files from all devices or select **No** to prevent AI-Scripts from collecting system log files.

5. (Optional) Select the **Apply to all Service Now managed devices** check box to configure the AI-Scripts parameters on all devices managed by Service Now.

6. (Optional) Select the **Schedule Configuration on selected device(s) at specified time** check box to schedule a date and time for configuring the AI-Scripts parameters.

7. Click **Submit**.

   If you have provided a schedule to configure the AI-Scripts parameters, Service Now configures the AI-Scripts parameters at the scheduled time. Otherwise, Service Now creates a job for configuring the AI-Scripts parameters on the selected devices immediately after you click Submit.

RELATED DOCUMENTATION

Installing an Event Profile on a Device by Using Service Now | 156

Adding a Script Bundle to Junos Space Service Now | 226

AI-Scripts Overview | 21

Deleting a Device from Junos Space Service Now

Junos Space Service Now provides the Delete option on the Actions list of the Service Now Devices page to delete a device from Junos Space Service Now database. When you delete a device, the device is deleted only from the Junos Space Service Now database along with its related incidents and JMBs. The device is not deleted from Junos Space Network Management Platform.

When you delete a device that has AI-Scripts installed on it from Service Now, the AI-Scripts package is automatically uninstalled from the device.

NOTE:

- If you uninstall a device from the Junos Space Platform first, you need to manually uninstall AI-Scripts from the device.

To delete a device from Service Now:

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

   The Service Now Devices page lists the Service Now devices.

2. Select one or more devices that you want to delete, and click **Delete** on the **Actions** list or the right-click menu.

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

3. Select the **Delete device(s) even if AI-Scripts un-installation fails** check box to delete the device from Service Now even if the uninstallation of AI-Scripts fails on the device.

   If you do not select this option, the device is not deleted from Service Now if the uninstallation of AI-Scripts fails on the device.

4. Click **Delete**.

   Service Now deletes the selected devices from the Service Now database and does not display it on the Service Now Devices page.

RELATED DOCUMENTATION

Service Now Devices Overview | 147

Associating Devices with a Device Group

Junos Space Service Now provides the Associate Device Groups option on the Actions list of the Service Now devices page to can associate devices with device groups. Associating devices with device groups helps you group devices under different site IDs.

If Service Now is configured to work in the Partner Proxy mode, you can combine devices that are directly managed by Service Now and devices from an end customer in a single Service Now device group. Alternately, you can create a device group for each end customer and associate them to Service Now

organizations dedicated to each end customer. This kind of grouping enables you to track and organize technical support cases for a single end customer using different organizations (site IDs).

To associate devices with a 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** list 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

- Device group Overview

Assigning an Auto Submit Policy to a Device

Auto submit policies allow Service Now to submit incidents automatically to Juniper Support Systems (JSS) or Service Now partner for creating cases. To assign auto submit policies to devices, you must first create them. For information on creating auto submit policies, see “Creating an Auto Submit Policy” on page 239
.

To assign an auto submit policy to a device:

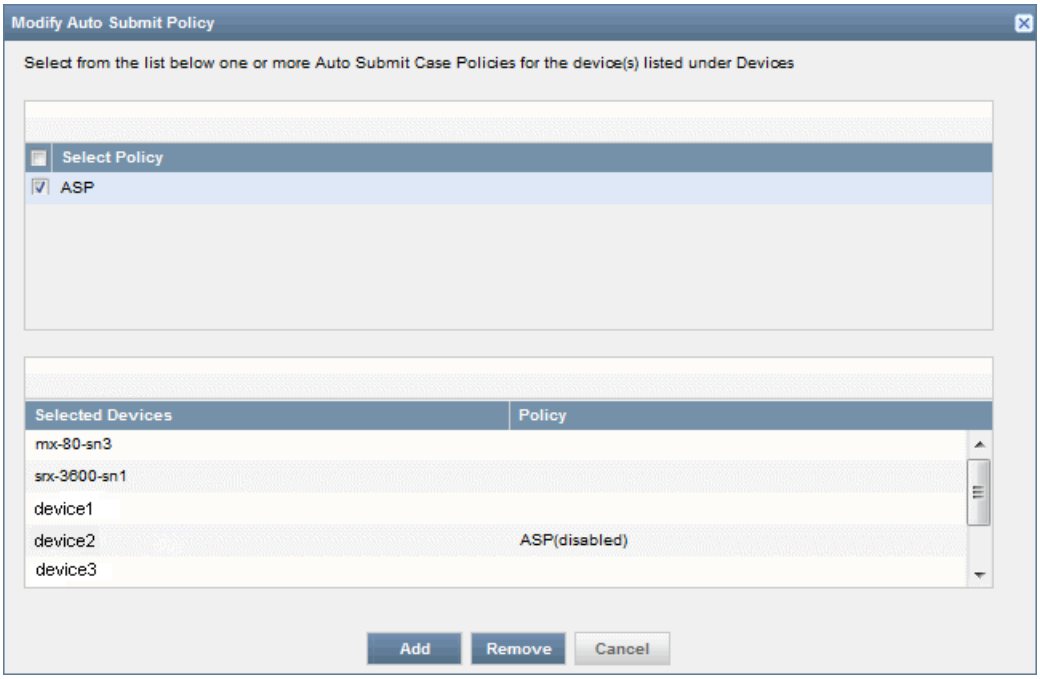
1. From the Service Now navigation tree, select **Administration** > **Service Now Devices**.

   The Service Now Devices page appears.

2. Select the devices for which you want to assign auto submit policies, and select **Modify Auto Submit Policy** from either the **Actions** list or the right-click menu.

   The **Modify Auto Submit Policy** dialog box appears and displays all the available auto submit policies and selected devices.

Figure 24: Modify Auto Submit Policy Page



3. Under the Select Policy section, select the auto submit policies that you want to assign to the selected devices.

> **TIP:** Click the check box next to Select Policy to select all auto submit policies for assigning to the selected devices.

4. To assign auto submit policies to selected devices, click **Add**.

> **TIP:** To remove an assigned policy from the devices, select the policy and click **Remove**.

The Service Now Devices page appears. Service Now displays the auto submit policies to which a device is assigned in the auto submit policy column.

5. (Optional) To verify your changes, navigate to **Administration** > **Auto Submit Policy** and view the list of devices assigned to the auto submit policies.

RELATED DOCUMENTATION

Service Now Auto Submit Policy Overview | 237
Adding Devices to Junos Space Service Now | 155
Service Now Devices Overview | 147
Collecting RSI and System Log Files | 187

Generating an On-Demand Incident

By using Junos Space Service Now, you can create Juniper Message Bundles (JMBs) for devices without having to wait for an event to occur on the device. These JMBs are called on-demand incident JMBs. On-demand JMBs can be generated by AI-scripts installed on devices or by Service Now. The on-demand JMBs generated by Service Now are referred to as off-box on-demand JMBs.

When you submit an on-demand incident to the device, 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 the type of incident and the remote procedure calls (RPCs) used to trigger the incident.

Service Now automatically submits these JMBs to the Juniper Support Systems (JSS) for creating a case. To avoid submitting incidents automatically, clear the **Automatically Submit Cases** check box present on the On-demand Incident dialog box displayed while creating the on-demand JMB.

NOTE:

- To create an on-demand incident, AI-Scripts Release 3.2 R1 or later must be installed on the device.
- You cannot create on-demand incidents for Juniper Networks QFX3000 Series and EX-XRE200 devices.
- You cannot create an on-demand incident for a device if the device is not associated with a device group.

Starting Junos Space Service Now 17.1R1 release, you can associate a new on-demand incident with technical support cases that are not closed. When an incident is associated with a case, the ID of the case is displayed in the Case Details tab of the Incident Details page and the Incidents page displays the Status of the incident as **Case Associated** along with the case ID with which the incident is associated. The attachments and log files of the incident are uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode) and associated with the related case.

NOTE:

- To associate an incident to a case, the case should not be in the Closed state.
- Once an incident is associated with a case, the association cannot be undone.
- An incident in one domain can be associated with a case assigned to another domain. A case can be associated with multiple domains.

To generate an on-demand incident:

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

   The Service Now Devices page appears.

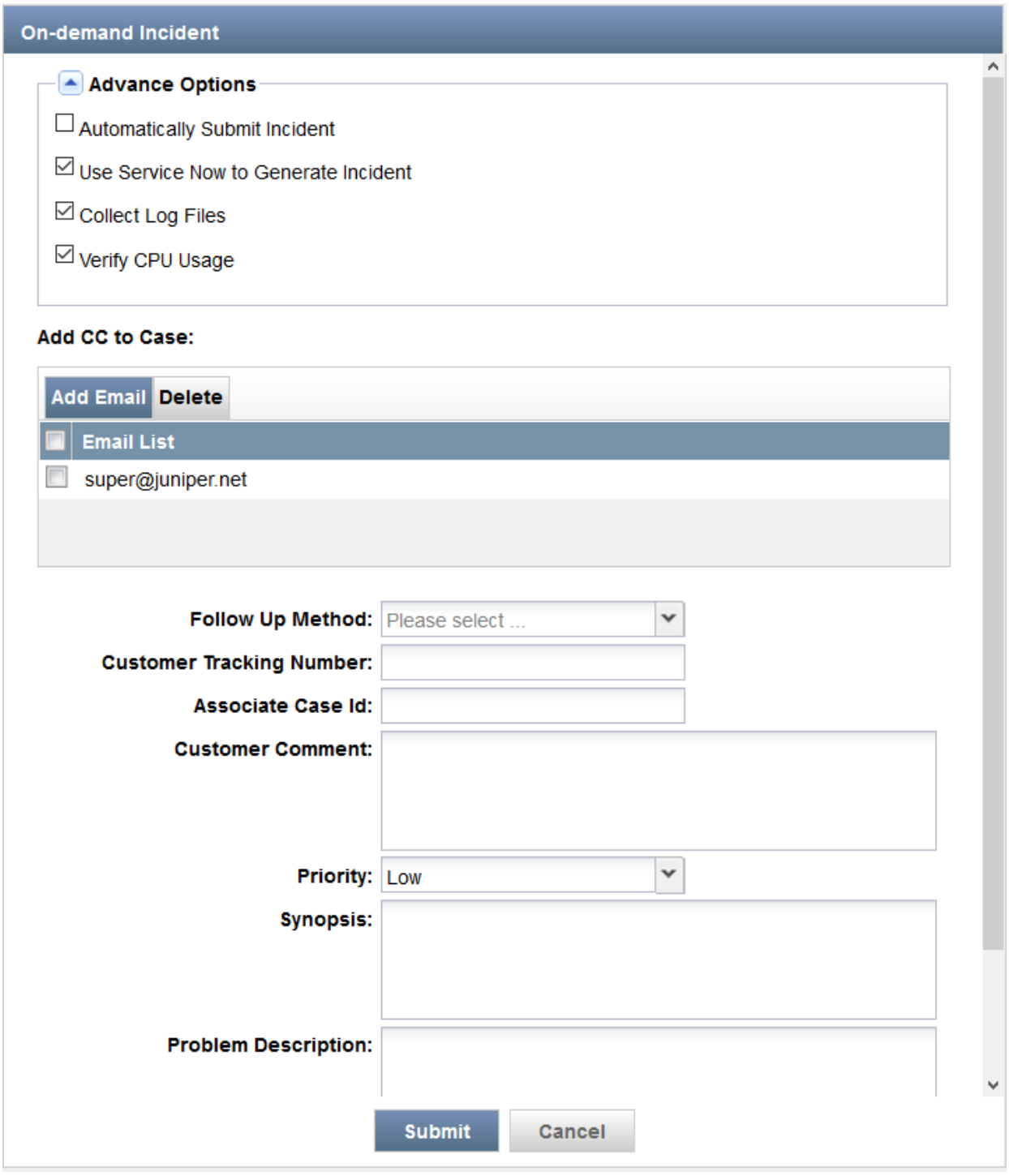
2. On the Service Now Devices page, select the device for which you want to generate an on-demand incident.

3. From the Actions list or the right-click menu, select **Device Operations > Create On-Demand Incident**..

   You can create on-demand incidents for up to five devices simultaneously.

   The On-demand Incident dialog box appears as shown in Figure 25 on page 176.

Figure 25: On-demand Incident Dialog Box



4. (Optional) At the top of the On-demand Incident dialog box, clear the **Automatically Submit Incident** check box to avoid submitting incidents to JSS or Service Now partner automatically, or to associate the incident with a technical support case.

> **NOTE:** The **Automatically Submit Incident** check box is selected by default.

5. (Optional) Select **Use Service Now to Generate Incident** to generate on-demand JMBs by using the off-box feature.

   If you select this option, the Incidents page within Service Central displays the incident type as off-box for on-demand incidents.

   Selecting the **Use Service Now to Generate Incident** check box displays the following options:

   a. **Collect Log Files**: Specifies if log files should be collected for the JMB.

      By default, the check box is selected and log files are collected for an off-box on-demand JMB. Clear the check box to avoid collecting log files for off-box on-demand JMBs.

   b. **Verify CPU Usage**: Specifies if load average values and ideal time of the CPU should be checked before generating the off-box on-demand JMB.

      By default, this check box is selected. If the average load and ideal time of the CPU are not within the limits defined in Table 16 on page 177, the off-box on-demand JMB is not generated and an error message is displayed. Service Now determines the CPU load average from the output of the **get-system-uptime-information** command and the CPU idle time from the output of the **get-route-engine-information** command.

      Table 16: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs

Device	CPU Load Average	CPU Ideal Time
MX240, MX480, MX960, MX120, MX320	< 2	> 15
Other Supported Devices	< 1	> 15

> **NOTE:** The Collect Log Files and Verify CPU Usage fields are not visible on the On-demand Incidents page if Service Now is operating in the End Customer mode.

6. Under Email List, click the **Enter Email Id** check box to enter an e-mail ID in the user@example.com format.

   Service Now sends a copy of the on-demand incident to the configured e-mail IDs.

7. (Optional) To add or delete multiple e-mail IDs, use the **Add Email** or **Delete** buttons respectively.

8. Select how updates about the case should be received from the **Follow Up Method** list. The available options are—Email Full Text Update, Email Secure Web Link, and Phone Call.

9. Enter the customer tracking number in the **Customer Tracking Number** field.

   Customer tracking number is a user-defined number assigned for tracking incidents and cases.

10. (Optional) To associate the on-demand incident with an existing technical support case, enter the Case ID of the technical support case in the **Associate Case Id** field.

    NOTE:
    - You can associate an on-demand incident with a technical support case only if the case is in the open state.
    - This field is visible only when the Automatically Submit Incident check box is not selected.

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

    The customer comment along with incident information appears as case notes (incident information listed first followed by the customer comment) in Case Manager. Service Now auto-generates the incident information and sends the incident information and customer comment to Case Manager.

    Total number of characters allowed in a customer comment is 38000.

    NOTE: This field is visible only when the Automatically Submit Incident check box is not selected.

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

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

13. In the **Synopsis** field, enter a synopsis of the on-demand incident.

    The maximum number of characters allowed in the Synopsis field is 1028.

    NOTE: The values for the fields listed in step 6 through step 12 are already defined on the basis of the incident that is generated by the selected profile. You can modify these values if needed.

14. In the **Problem Description** field, enter a description of the on-demand incident.

    The maximum number of characters allowed in the Problem Description field is 1028.

15. (Optional) If you want to schedule generating the on-demand incident at a later time, select the **Schedule at a later time** check box and enter the date and time for the schedule.

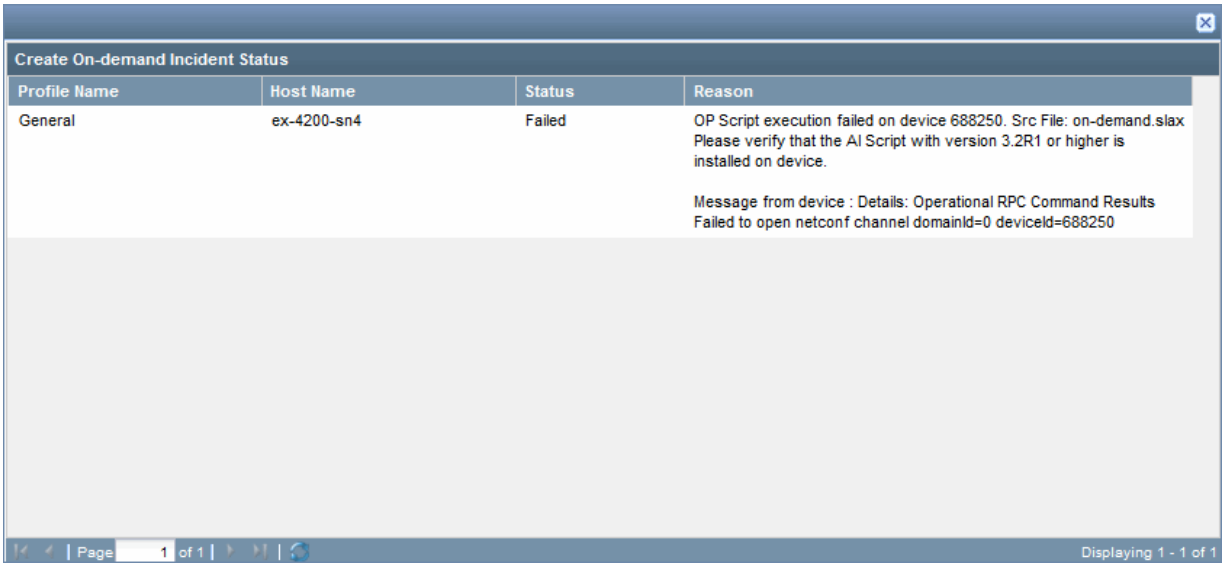
    If you do not schedule a time, the on-demand incident is created immediately after you complete configuring the on-demand incident.

16. Click **Submit**.

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

    You can click the job ID link to go to the create on-demand incident job on the Jobs page. Double-click the job to open the Create On-demand Incident Status dialog box (shown in Figure 26 on page 179), which displays information about the job such as the profile used in the incident, hostname of the device running Junos OS, job status, and reason for the incident.

Figure 26: Create On-demand Incident Status Dialog Box



Release History Table

Release	Description
17.1R1	Starting Junos Space Service Now 17.1R1 release, you can associate a new on-demand incident with technical support cases that are not closed. When an incident is associated with a case, the ID of the case is displayed in the Case Details tab of the Incident Details page and the Incidents page displays the Status of the incident as **Case Associated** along with the case ID with which the incident is associated.

RELATED DOCUMENTATION

Service Now Incidents Overview

Generating an On-Demand Device Snapshot

Junos Space Service Now provides the *Create On-Demand Device Snapshots* action for managed devices to generate off-box on-demand device snapshots or informational Juniper Message Bundles (iJMBs) on managed devices. You can choose to automatically upload the iJMB to Juniper Support System (JSS) or the Service Now partner (in case Service Now is operating in the End Customer mode).

NOTE: You cannot create an on-demand device snapshot for a device if the device is not associated with a device group.

To generate an on-demand device snapshot:

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

   The Service Now Devices page appears.

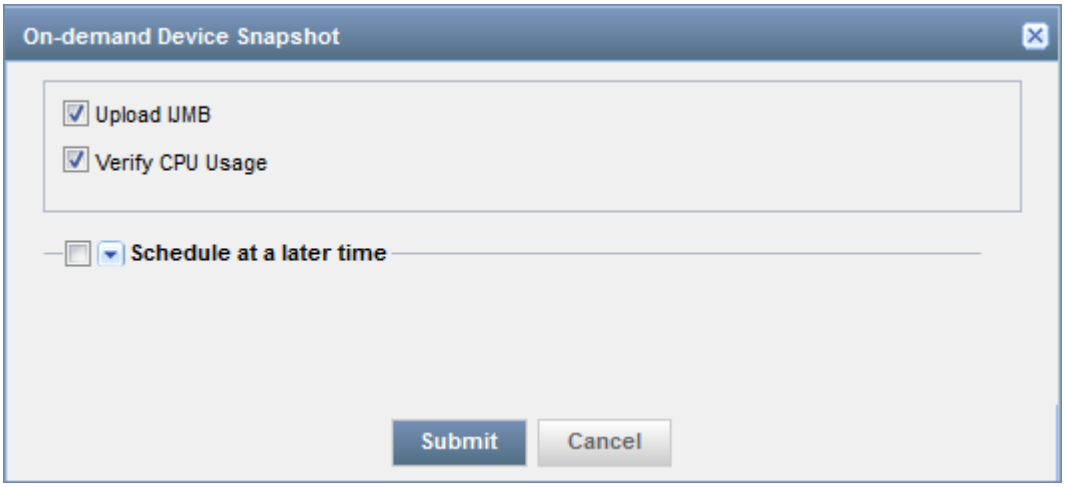
2. On the Service Now Devices page, select one or more devices for which you want to generate an on-demand device snapshot.

   NOTE: You can create on-demand incidents for up to five devices simultaneously.

3. From the Actions list, select **Device Operations > Create On-Demand Device Snapshots**. Alternatively, right-click the selected devices and select **Device Operations > Create On-Demand Device Snapshots**.

   The On-demand Incident dialog box appears as shown in Figure 27 on page 181.

Figure 27: On-demand Incident Dialog Box



4. (Optional) Clear the **Upload iJMB** check box to prevent Service Now from automatically uploading the to Juniper Support Systems (JSS) or Service Now partner.

   By default, the check box is selected and iJMBs are automatically uploaded to JSS or Service Now partner..

5. (Optional) Clear the **Verify CPU Usage** check box to avoid Service Now from checking the load average value and ideal time of the device CPU before generating the iJMB.

   By default, this check box is selected. If the average load and ideal time of the CPU are not within the limits defined in Table 17 on page 181, the off-box on-demand JMB is not generated and an error message is displayed. Service Now determines the CPU load average from the output of the **get-system-uptime-information** command and the CPU idle time from the output of the **get-route-engine-information** command.

   Table 17: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs

Device	CPU Load Average	CPU Ideal Time
MX240, MX480, MX960, MX120, MX320	< 2	> 15
Other Supported Devices	< 1	> 15

6. (Optional) If you want to schedule generating the on-demand incident at a later time, select the **Schedule at a later time** check box and enter the date and time for the device snapshot be generated.

7. Click **Submit**.

Service Now creates a job for generating the device snapshot and displays the job ID as a link in the Job information dialog box.

8. Click the *job ID* link to go to the Create on-demand Device Snapshot job on the Jobs page.

9. Double-click the job to open the Create On-demand Incident Status dialog box to view the status of the create on-demand device snapshot job.

   Service Now lists the device snapshot on the Device Snapshots page.

RELATED DOCUMENTATION

Service Now Devices Overview | 147

Assigning an Auto Submit Policy to a Device | 172

Service Now Incidents Overview

Generating an RMA Incident for a Device

You can use the off-box feature in Service Now to generate Return Materials Authorization (RMA) incidents for a device. With the off-box feature, Service Now generates RMA incidents using the preloaded **directive.rc** file. In a Service Now operating in the Partner Proxy mode, you cannot create an RMA incident for end-customer devices by using the off-box feature..

> **NOTE:** Currently, this feature is not supported on devices that are not associated with a device group.

Starting Junos Space Service Now 17.1R1 release, you can associate a new RMA incident with technical support cases that are not closed. When an incident is associated with a case, the ID of the case is displayed in the Case Details tab of the Incident Details page and the Incidents page displays the Status of the incident as **Case Associated** along with the case ID with which the incident is associated. The attachments and log files of the incident are uploaded to Juniper Support Systems (JSS) or Service Now partner (in case of End Customer mode) and associated with the related case.

NOTE:

- To associate an incident to a case, the case should not be in the Closed state.
- Once an incident is associated with a case, the association cannot be undone.
- An incident in one domain can be associated with a case assigned to another domain. A case can be associated with multiple domains.

To generate an RMA incident for a device:

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

   The Service Now Devices page appears.

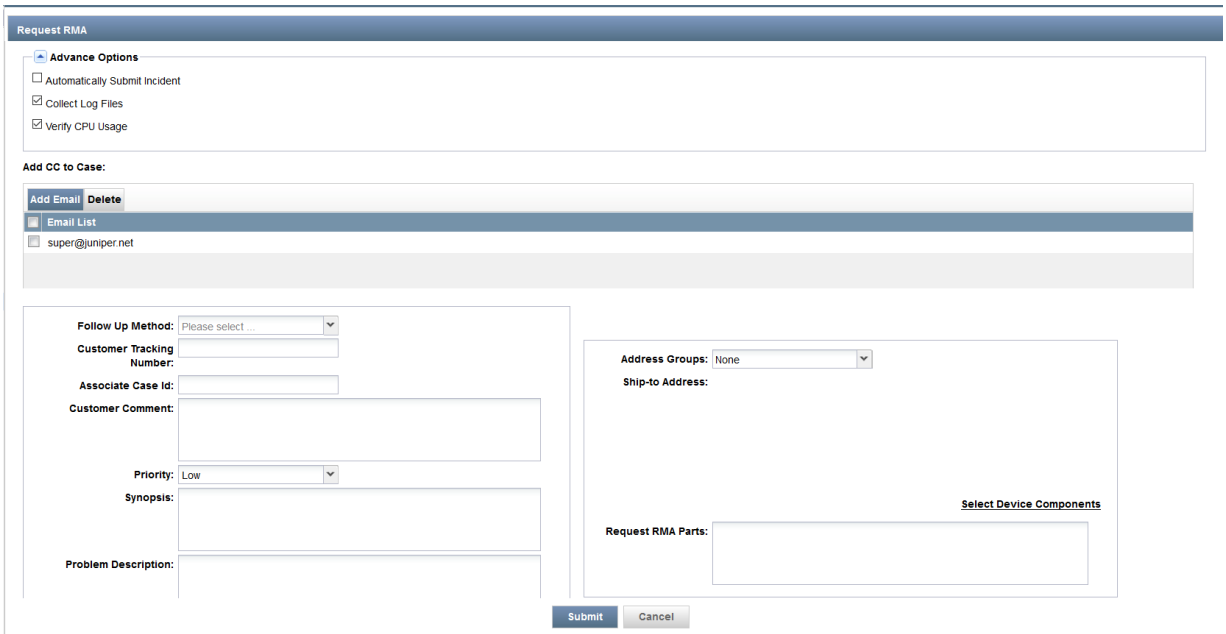
2. On the Service Now Devices page, select the device for which you want to generate an RMA incident.

3. From the Actions list or the right-click menu, select **Device Operations > Request RMA**. .

   NOTE: Currently, Service Now supports requesting RMA incidents for only one device at a time.

   The Request RMA page appears as shown in Figure 28 on page 183.

Figure 28: Request RMA page



4. (Optional) At the top of the Request RMA page, clear the **Automatically Submit Incident** check box if you do not want to submit RMA incidents automatically to Juniper Support Systems (JSS) or Service Now partner, or associate the incident with a technical support case..

   NOTE: The **Automatically Submit Incident** check box is selected by default.

5. (Optional) Clear the **Collect Log Files** check box if you do not want to collect log files for the RMA JMBs.

6. (Optional) Clear the **Verify CPU Usage** if you do not want load average values and ideal time of the CPU to be checked before generating the Request RMA JMBs.

   If the average load and ideal time of the CPU are not within the limits defined in Table 18 on page 184, the RMA JMBs are not generated and an error message is displayed. Service Now determines the CPU load average from the output of the **get-system-uptime-information** command and the CPU idle time from the output of the **get-route-engine-information** command.

   Table 18: Values for CPU Load Average and CPU Ideal Time for generating Off-box On-demand JMBs

Device	CPU Load Average	CPU Ideal Time
MX240, MX480, MX960, MX120, MX320	< 2	> 15
Other Supported Devices	< 1	> 15

7. Under Email List, click the **Enter Email Id** check box to enter an e-mail ID in the user@example.com format.

   Service Now sends a copy of the RMA incident to the configured e-mail IDs.

8. (Optional) To add or delete e-mail IDs, use the Add Email or Delete buttons respectively.

9. From the **Follow Up Method** list, select the mode for receiving updates about the case.

   The available options are—Email Full Text Update, Email Secure Web Link, and Phone Call.

10. Enter the customer tracking number in the **Customer Tracking Number** field.

    Customer tracking number is a user-defined number assigned for tracking incidents and cases.

11. (Optional) To associate the RMA incident with an existing technical support case, enter the Case ID in the **Associate Case Id** field.

NOTE:

- You can associate an RMA incident with a technical support case only if the case is in the open state.
- This field is visible only when the Automatically Submit Incident check box is not selected.

12. (Optional) Enter a comment for associating the selected incidents with the case in the **Customer Comment** text field.

    The customer comment along with incident information appear as case notes (incident information listed first followed by the customer comment) in Case Manager. Service Now auto-generates the incident information and sends the incident information and customer comment to Case Manager.

    Total number of characters allowed in a customer comment is 38000.

    NOTE: This field is visible only when the Automatically Submit Incident check box is not selected.

13. From the **Priority** list, select the priority of the case.

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

14. In the **Synopsis** field, enter a synopsis of the RMA incident.

    The maximum number of characters allowed in the Synopsis field is 1028.

15. In the **Problem Description** field, enter a description of the RMA incident.

    The maximum number of characters allowed in the Problem Description field is 1028.

16. Select the address group from the **Address Groups** list.

    The address group indicates the address to which the replacement part should be shipped.

    The Address Groups list lists all the address groups configured in Service Now and None. None indicates that no address group is associated with this request.

    The **Ship-to Address** field is auto-populated with the address configured in the selected address group.

17. Click the **Select Device Components** link.

    The Device Physical Inventory Components page that appears displays the device parts with an option to select device parts or components. The selected components appear in the **Request RMA Parts** text box.

18. (Optional) If you want to schedule generating the RMA incident at a later time, select the **Schedule at a later time** check box and enter the date and time for the schedule.

19. Click **Submit**.

    Service Now initiates a job to create an RMA incident.

    If you have scheduled a time for creating the RMA incident, Service Now initiates the process to create the RMA incident at the scheduled time.

Release History Table

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

RELATED DOCUMENTATION

Service Now Incidents Overview

Verifying the Connection Between a Device and the SFTP Server

Junos Space Service Now uploads core files generated as a part of a JMB to an SFTP server.When there is an issue in uploading core files, you can verify the connection between the devices and the SFTP server.

NOTE: You cannot verify the connection between a device and the SFTP Server by using Service Now when Service Now is operating in the End Customer mode.

To verify the connection between the device and the SFTP server:

1. From the Service Now navigation tree, select **Administration** > **Service Now devices**. The Service Now Devices page appears.

2. Select the device for which you want to verify the connection with the SFTP server, and select **Check FTP Server** from either the **Actions** list or the right-click menu.

The Check FTP Server Access dialog box appears.

3. Select the device, and click **Submit**.

   The Alert dialog box appears with the Job ID.

   Click the *job ID* to go to the Job Management page and monitor the connectivity status.

RELATED DOCUMENTATION

Configuring Core file Upload

Configuring SFTP Server for Uploading Core Files Generated for Events | 84

Updating Core File Upload Configuration for an End Customer | 132

Collecting RSI and System Log Files

Junos Space Service Now provides the Configure File Collections option to configure the interval during which a Request Support Information (RSI) command can be executed on a device to gather device configuration information. For example, you can set the RSI command to be executed every two hours. When you configure an interval for collecting RSI, Service Now executes the RSI command only once during the configured interval to collect RSI. For events that occur within the configured interval after RSI is collected, Service Now uses the already collected RSI in the JMB of those events.

> **NOTE:** Service Now executes the RSI brief command on devices running subscriber management services instead of the regular RSI command to avoid impacting the performance of device CPU.
>
> The RSI brief command does not execute the **detail** option due to which size of the output is smaller as compared with the output of regular RSI command.

The following example illustrates how RSI is collected from a device. In this example, the following considerations are made:

- Configured interval for collecting RSI: 1hr

- Time at which RSI was last executed: 1:00 PM

Time of Event	RSI Executed	Comment
1:30 PM	No	RSI is not collected at 1:30 PM as one hour has not yet elapsed since RSI was last collected at 1:00 PM.
1:59 PM	No	RSI is not collected at 1:59 PM as one hour has not yet elapsed since RSI was last collected at 1:00 PM.
2:00 PM	Yes	RSI is collected at 2:00 PM as one hour has elapsed since RSI was last collected at 1:00 PM.
2:01 PM	No	RSI is not collected at 2:01 PM as one hour has not yet elapsed since RSI was last collected at 1:00 PM.
4:30 PM	Yes	RSI is collected at 4:30 PM as two-and-a-half hours have elapsed since RSI was last collected at 2:00 PM. The configured interval to collect RSI is 1hr.
4:35 PM	No	RSI is not collected at 4:35 PM as one hour has not yet elapsed since RSI was last collected at 4:30 PM.
5:30 PM	Yes	RSI is collected at 5:30 PM as one hour has elapsed since RSI was last collected at 4:30 PM.

NOTE:

- The icon, if present in the device row (next to the device's organization), indicates that while copying a JMB from the device to Service Now, one or more JMB files, such as attachments or log files, are not deleted from the device.

  If you place the cursor on the icon, the files that are not deleted are displayed. You must manually delete these files from the device.

- From AI-Scripts Release 4.0 onward, the Attachment section of a JMB contains commands executed in response to an event and links that you can click to view or download the command output.

- We recommend that you configure RSI collection at least once by using Service Now to ensure proper generation of the RSI attachment for a JMB.

To configure the interval for collecting RSI and system log files:

1. In the Service Now navigation tree, select **Administration > Service Now Devices**.

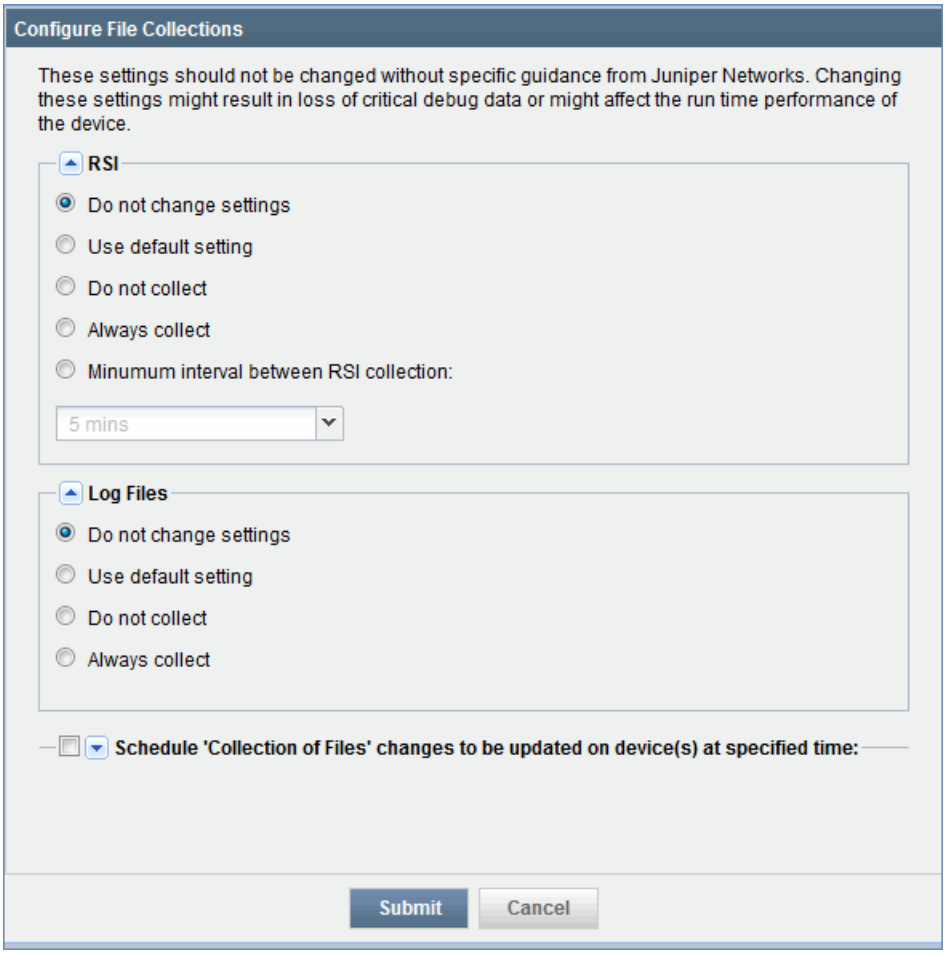
   The Service Now Devices page appears.

2. On the Service Now Devices page, select the device for which you want to collect RSI and system log files.

3. From the Actions list or right-click menu, select **Configure File Collection**.

   The Configure File Collections dialog box appears as shown in Figure 29 on page 189.

Figure 29: Configure File Collections Dialog Box



4. In the RSI section of the Configure File Collections dialog box, select one of the following:

   - **Do not change settings** to leave the settings for collecting RSI as is. This option is selected by default.

     Using this dialog box, you can choose to configure the interval for collecting only the RSI or log files. If you want to configure collecting only the log files without changing the configuration for collecting RSI files, select this option.

For all devices, by default, Service Now is configured to collect RSI every five minutes. However, the following exceptions apply:

- Service Now is configured to collect RSI once every 15 minutes for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.
- Service Now is configured to not collect RSI for the following devices:
  - ACX Series—ACX1000 and ACX1100
  - EX Series—EX2200 and EX3300
  - SRX Series—SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650

- **Use default setting** to collect RSI from the device for an event if five minutes have passed since RSI was last collected from that device
- **Do not collect** if you do not want to collect RSI for any event that occurs on the device
- **Always collect** to always collect RSI for all events that occur on the device
- **Minimum interval between RSI collection** to configure the minimum time interval for collecting RSI between consecutive events. If you select this option, select the time interval from the drop-down list provided below this option.

5. In the Log Files section of the Configure File Collections dialog box, select one of the following:

   - **Do not change settings** to leave the settings for collecting system log files as is. This option is selected by default.

     By using this dialog box, you can choose to configure the interval for collecting only the RSI or system log files. If you want to configure collecting only RSI without changing the configuration for collecting system log files, select this option. By default, Service Now is configured to collect system log files for every event.

   - **Use default setting** to collect system log files for every event that occurs on the device
   - **Do not collect** if you do not want to collect system log files for any event that occurs on the device
   - **Always collect** to collect system log files for every event that occurs on the device

6. (Optional) If you want to schedule this configuration for a later time, select the **Schedule 'Collection of Files' changes to be updated on device(s) at specified time:** check box and select a date and time for the schedule from the list.
7. Click **Submit**.

   A job is created to save the configuration and the job ID is displayed in the Job Information dialog box. If you have scheduled a time, the job for creating the on-demand incident is initiated at the scheduled time.

8. (Optional) In the Job Information dialog box, click the job ID link to view the status of the job.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Configuring BIOS Validation for Verifying BIOS Integrity of a Device

By configuring BIOS validation, you enable Service Now to collect data from a device running Junos OS for verifying BIOS integrity of the device. If you are configuring BIOS validation for the first time on a device or after discovering and adding devices to Service Now, you are provided with the BIOS legal notice. You must accept the legal notice before you configure BIOS validation on Service Now devices.

To configure BIOS validation on a device for verifying BIOS integrity:

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

   The Service Now Devices page appears.

2. Select a device on which you want to configure BIOS validation.

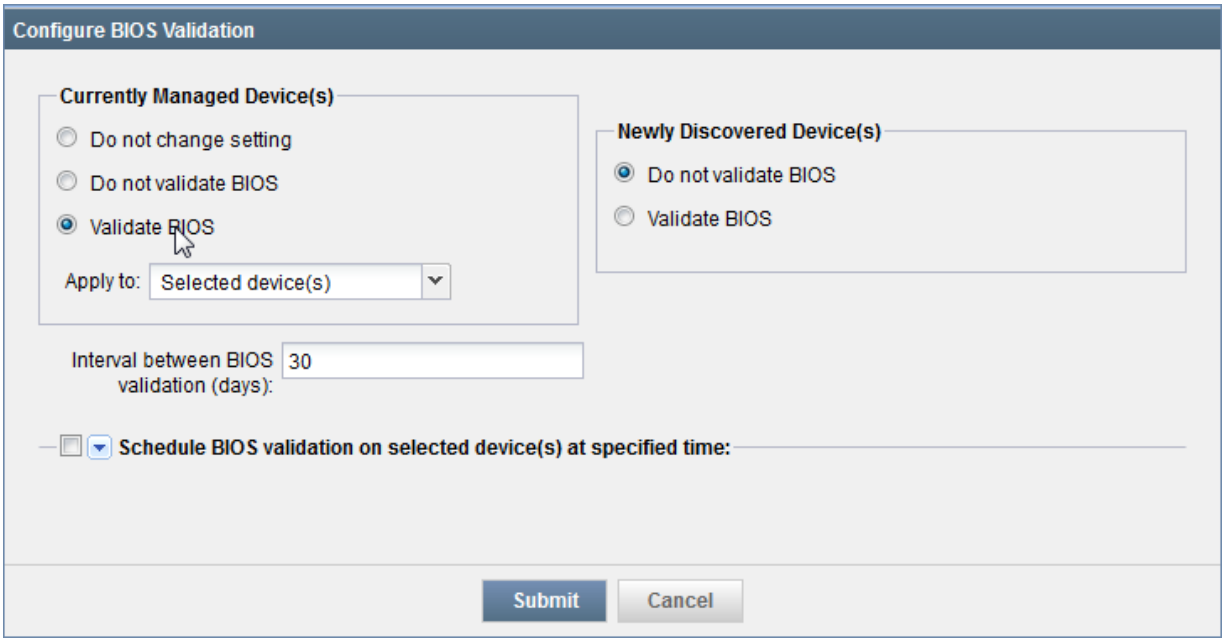
3. From the Actions list, select **Device Analysis > Configure BIOS Validation**. Alternatively, right-click the device and select **Device Analysis > Configure BIOS Validation**.

   The Configure BIOS Validation dialog box appears.

   NOTE: The BIOS legal notice appears when you configure BIOS validation for the first time or after you remove and add devices back to Service Now.

   Read and accept the legal notice. The Configure BIOS Validation dialog box appears after you accept the legal notice.

Figure 30: Configure BIOS Validation Dialog Box



4. Perform one of the following tasks:
   - If the device is AI-Scripts enabled (that is, AI-Scripts is installed on the device), under Currently Managed Device(s), select one of the following options:
     - **Do not change setting**—Leaves the settings for collecting data for BIOS validation as is. This option is selected by default.

       By default, Service Now is not configured to collect data for BIOS validation.
     - **Do not validate BIOS**—Disables BIOS validation
     - **Validate BIOS**—Enables BIOS validation
     - From the **Apply to** drop-down menu, select one of the following options:
       - **Selected Devices**—Configures BIOS validation on selected devices only
       - **All currently managed devices**—Configures BIOS validation on all devices currently managed by Service Now
   - If the device is a newly discovered device, select one of the following options:
     - **Do not validate BIOS**—Disables BIOS validation
     - **Validate BIOS**—Enables BIOS validation
5. If you select **Validate BIOS**, enter the number of days between successive BIOS validations in the **Interval between BIOS validation (days):** text box.

The number of days between BIOS validations on a device should be between 15 and 30 days. 30 days is the default setting.

6. (Optional) Select the **Schedule BIOS validation on selected device(s) at specified time:** check box to configure the date and time for collecting BIOS data.

7. Click **Submit** to configure BIOS validation or **Cancel** to cancel the configuration.

   When you click Submit, Service Now creates a job is created and the Job ID is displayed on the Job Status dialog box.

8. Click the Job ID to view the details and status of the job.

   The Success status of the Configure BIOS validation job indicates that a cron job is initiated on the device to collect BIOS data. The cron job is set to execute once a day at 2:00 AM (local time of the device). A BIOS validation record is created on Service Now a few minutes after the cron job is initiated. You can view the BIOS validation record on the job BIOS Validations page.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Exporting Device Data in CSV and Excel Formats

Junos Space Service Now provides the Export Devices option on the Actions list of the Service Now devices page to export Service Now device data in CSV or Excel file formats.

Service Now exports the following information about a device:

- Host name of the device
- IP address of the device
- Device group to which the device is assigned
- Organization associated with the device
- Organization associated with the end customer device when the device is an end customer device (
- Product family to which the device belongs
- Routing software installed on the device
- Serial number of the device

- Version of the routing software
- AI-Scripts version installed on the device
- Event profile installed on the device
- Date and time the event profile was installed on the device
- Location of the device
- Address where the RMA parts for the device should be shipped
- Domain to which the device is assigned
- Auto submit policy assigned to the device
- Whether or not the device is operating in the maintenance mode
- RSI file configuration of the device
- Log file configuration of the device

To export the device data in CSV or Excel format:

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

   The Service Now Devices page appears.

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

   > **TIP:** To export data of all devices in Service Now, select the check box on the header of the table on the Service Now devices page.

   The **Export Devices** dialog box is displayed.

3. Export the device information:
   - Click the **Export Devices in CSV Format** to export the device data in CSV format.
   - Click the **Export Devices in Excel Format** to export the device data in Excel format.

   The browser displays the dialog box to open or save the file

4. Open or save the file at a desired location.

RELATED DOCUMENTATION

Service Now Devices Overview | 147

Deleting a Device from Junos Space Service Now | 170

Assigning an Auto Submit Policy to a Device | 172

Exporting Inventory Information in CSV Format

A Service Now partner can export a customer's device inventory information to CSV or Excel file format.

Service Now exports the following inventory information to the CSV or Excel file—device name, item, model number, part number, serial number, contract number, service SKU, contract start, contract end and description.

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

To export the inventory information:

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

   The Service Now Devices page appears.

2. - To export inventory of selected devices, select the device and click **Export Inventory Information** either from the **Actions** list or the right-click menu.
   - To export inventory of all devices in Service Now, select **Export Inventory Information** either from the **Actions** list or the right-click menu.

   The Export Inventory Information dialog box is displayed.

3. Export the inventory information:
   - Click the **Export Inventory Information in CSV format** link to export the inventory information for selected devices to a CSV file.
   - Click the **Export All Inventory Information in CSV format** link to export the inventory information for all devices in Service Now to a CSV file.
   - Click the **Export Inventory Information in Excel format** link to export the inventory information for selected devices to an Excel file.
   - Click the **Export All Inventory Information in Excel format** link to export the inventory information for all devices to an Excel file.

   The Export Inventory Job Status dialog box appears and shows the job status.

4. After the job is complete, click the **Download** link to either open or save the CSV or Excel file.

RELATED DOCUMENTATION

Service Now Devices Overview | 147

Viewing Incidents Created for a Device

Junos Space Service Now creates incidents when it receives a JMB from a device. You can view the incidents on the Incidents page of the Service Central workspace.

To view incidents created in Service Now:

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

   The Service Now Devices page lists the Service Now devices.

2. Select a device to view the incidents that Service Now has created.

   NOTE: Currently, Service Now allows you to select only one device at a time.

3. Select **View incidents** from either the **Actions** list or the right-click menu.

   The Incidents page displays the incidents detected for the selected device. For incident details, see *Service Now Incidents Overview*.

   Alternatively, you can view all the incidents created for all devices on the Service Now dashboard.

RELATED DOCUMENTATION

Incidents Overview

Service Central Overview

Viewing Exposure for a Device

The Service Now Devices page displays an alert (!) icon before the Organization column of devices for which advisories (also known as Install Advisor or exposure) are issued for installing AI-Scripts.

The Install Advisor is an advisory created by Juniper Support Systems (JSS) to advice you of any issues with AI-Scripts on the Junos OS versions running on devices managed by Service Now. The advisory includes a number and link to the problem report (PR) that describes the issue, a message, product model, and information about the Junos OS and AI-Scripts version that have the issue.

Service Now retrieves advisories from JSS once every 24 hours and scans all the devices managed by it to check if the devices match the parameters (product model, Junos OS version, and AI-Scripts version) mentioned in the advisory. If there is a device matching the parameters specified in the advisory, Service Now displays an alert icon for that device on the Service Now Devices page. Clicking the alert icon displays a warning message indicating the device has known issues.

The alert icon is also displayed for a device when a version of AI-Scripts that has an advisory issued is selected for installing on the device.

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

To view advisory or exposure for a device:

1. On the Service Now navigation tree, select **Administration** > **Service Now Devices**.

   The Service Now Devices page appears.

2. Select the device that is susceptible (with the (!) icon) and click **View Exposure** from the **Actions** list or the right-click menu.

   The View Exposure page appears and displays the device name, product, version, PR, and PR synopsis.

3. Click the link in the PR column to view the issue and take suitable actions.

   Clicking the link opens the Problem Report Search tool and displays the details of the PR.

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

RELATED DOCUMENTATION

Service Now Devices Overview | 147

Moving a Device to Maintenance Mode

Starting Junos Space Service Now Release 15.1R1, Service Now provides the Maintenance Mode option on the Actions list to move a managed device to the maintenance mode. When a device is placed in the maintenance mode, event Juniper Message Bundles (eJMBs) are not generated on the device.

You cannot perform the following tasks when a managed device is placed in maintenance mode:

- Configure BIOS validation
- Configure product health checks
- Generate on-demand JMBs (by using AI-Scripts)
- Generate on-demand device snapshots

When operating in the End Customer mode, Service Now provides updates to the Service Now partner about the Service Now devices in maintenance mode once a day or whenever a device is moved to or out of the maintenance mode. A Service Now partner can view whether managed devices of Service Now end customers are in maintenance mode or not, but cannot move the devices of Service Now end customers to maintenance mode.

NOTE:

- Devices can be moved to maintenance mode only if AI-Scripts Release 5.0 or later is installed on the device.
- QFX Series devices in a QFabric cannot be moved to the maintenance mode.

To move a device to maintenance mode:

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

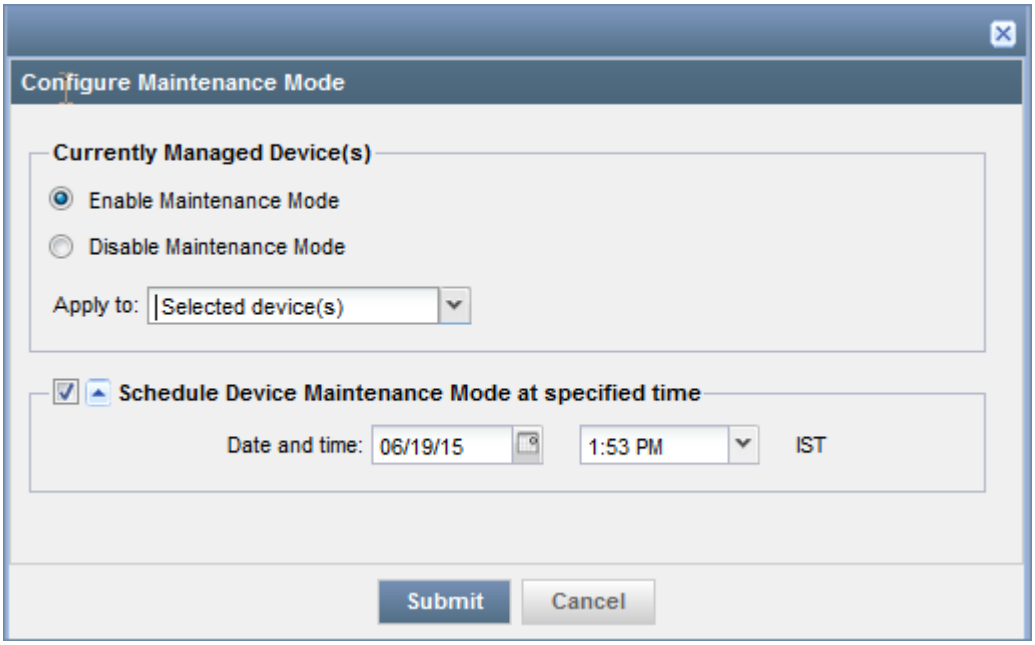
   The Service Now Devices page appears.

2. On the Service Now Devices page, select the device that you want to move to maintenance mode.

3. From the Actions l, select **Device Operations > Maintenance Mode**. Alternatively, right-click the device and select **Device Operations > Maintenance Mode**.

   The Configure Maintenance Mode dialog box appears as shown in Figure 31 on page 199.

Figure 31: Configure Maintenance Mode Dialog Box



4. On the Configure Maintenance Mode dialog box, do one of the following:
   - Click **Enable Maintenance Mode** to move the device to maintenance mode.
   - Click **Disable Maintenance Mode** to move the device out of maintenance mode.
5. From the **Apply to** drop-down list, select one of the following options:
   - **Selected device(s)** to move devices selected on the Service Now Devices page to the maintenance mode
   - **All managed devices in the current domain** to move all the managed devices in the current domain to maintenance mode.
6. (Optional) Select the **Schedule Device Maintenance Mode at Specified Time** to schedule the time to move devices to the maintenance mode.
7. Click **Submit** to move the device to the maintenance mode.

   The progress of the job to move the devices to the maintenance mode is displayed.
8. (Optional) Click the ***job Id*** link to view the progress of the job.

   After the device is moved to maintenance mode, the Service Now Devices page displays ON in the Maintenance Mode column of the device.

Release History Table

Release	Description
15.1R1	Starting Junos Space Service Now Release 15.1R1, Service Now provides the Maintenance Mode option on the Actions list to move a managed device to the maintenance mode.

RELATED DOCUMENTATION

Service Now Devices Overview | 147

10

CHAPTER

Configuring and Managing Event Profiles and Script Bundles

Service Now Event Profiles Overview | **203**

Adding an Event Profile to Junos Space Service Now | **210**

Cloning an Event Profile | **214**

Importing Event Profiles into Junos Space Service Now in XML Format | **219**

Deleting Event Profiles from Junos Space Service Now | **221**

Pushing an Event Profile to Devices | **221**

Setting an Event Profile as the Default Event Profile in Junos Space Service Now | **225**

Adding a Script Bundle to Junos Space Service Now | **226**

Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now | **227**

Deleting a Script Bundle from Junos Space Service Now | **228**

Displaying Devices Associated with an Event Profile | **229**

Exporting Events Data in Excel Format | **229**

Exporting Event Profiles from Junos Space Service Now in XML Format | **230**

Service Now Event Profiles Overview

An event profile is a set of event scripts, selected from an AI-Scripts bundle that you install on Junos Space Service Now devices. The event scripts in the event profile determine the events for which AI-Scripts generate an event Juniper Message Bundle (eJMB.

Juniper Networks ships the latest AI-Scripts bundle with Service Now and hence when you install Service Now, the latest AI-Scripts bundle is displayed on the Script Bundles page (**Administration > Event Profiles > Script Bundles**). 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 Junos Space Service Now" on page 226).

Service Now also has a default event profile that is associated with the default AI-Scripts bundle. For new Service Now installations or upgrades, Service Now associates the default event profile with the AI-Scripts bundle shipped with Service Now.

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. Service Now uses the default Scripts bundle to create a new event profile and selects the default event profile while installing an event profile on devices.

> **NOTE:** Read the KB article, https://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, the associated AI-Scripts bundle, set of included event scripts, and event script priorities. You can clone an event profile to create a new event profile by modifying a few attributes of the original event profile. After you make your modifications, you can save the cloned event profile and install it on devices on which the original event profile is installed. You can also install the new event profile on any device.

The priority of event policies in an event profile determine the priority shown in the JMBs generated for a Service Now event. Service Now allows you to export event data that is specific to an event profile to Excel format and delete event profiles that are not associated with devices.

You can view event profiles on the Event Profiles page (**Administration > Event Profiles**) as shown in Figure 32 on page 204. Table 19 on page 204 lists the information displayed on the Event Profiles page The default event profile is indicated by a unique icon. In Figure 32 on page 204, Base_Profile_3_7R1_ 2 is the default event profile.

Figure 32: View Event Profiles Page

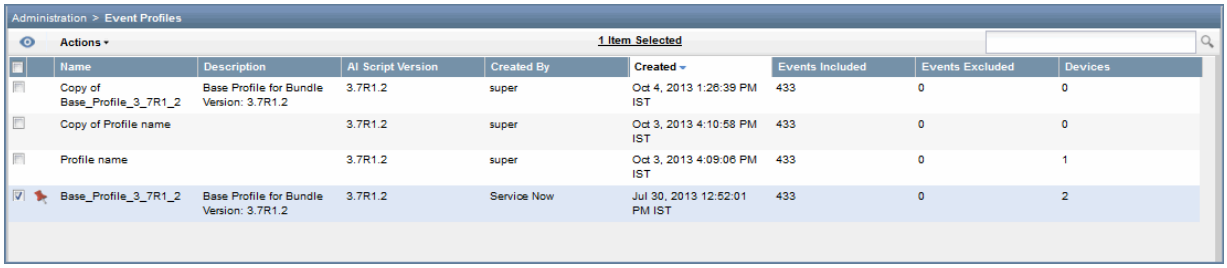


Table 19 on page 204 lists the parameters of event profiles.

Table 19: Event Profile Parameters

Parameter	Description
Name	Name of the event profile
Description	Description of the event profile
AI-Scripts Version	Version of AI-Scripts used to created the event profile
Created By	User who created the event profile
Created	Date and time when the event profile was created
Events Included	Number of events from the AI-Scripts bundle included in the event profile
Events Excluded	Number of events from the AI-Scripts bundle not included in the event profile
Total Events in Script Bundle	Number of events in the AI-Scripts bundle using which the event profile was created
Events with No Incidents	Number of events for which incidents have not been created
Total Incidents	Number of incidents that are created by using the event profile
Associated Devices	Number of devices on which the event policy is installed
Domain	Domain to which the event policy is assigned

Installing, Upgrading, or Uninstalling AI-Scripts on Managed Devices without Modifying Device Configuration Overview

Advanced Insight Scripts (AI-Scripts) provide the intelligence that managed devices need to automatically detect and report hardware and software failure or other functional abnormalities. For AI-Scripts to provide intelligence to a device, AI-Scripts must be installed and AI-Scripts configuration committed on a device running Junos OS.

Starting in Service Now Release 15.1R1, when AI-Scripts Release 5.0R1 is installed (or an earlier version is upgraded to Release 5.0R1) on the device for the first time, a static AI-Scripts configuration is pushed and commited on the device. The static configuration, once committed on the device, is used during successive installation or upgrade of AI-Scripts. This eliminates the need for pushing and committing AI-Scripts configuration for each AI-Scripts installation or upgrade.

The Static AI-Scripts comprises the following Junos OS commands:

```
set groups juniper-ais system scripts op file ais_change_perm.slax
set groups juniper-ais system scripts op file ais_core_perm.slax
set groups juniper-ais system scripts op file on-demand.slax
set groups juniper-ais system scripts op file remove-jais.slax
set groups juniper-ais system scripts op file ais_arc.slax
set groups juniper-ais system scripts op file ais-attach-file.slax
set groups juniper-ais system scripts op file stop-ais-now.slax
set groups juniper-ais system scripts op file ais_signalSN.slax
set groups juniper-ais system scripts op file ais_core_chm.slax
set groups juniper-ais system scripts op file ais_all_chm.slax
set groups juniper-ais system scripts op file att_signalSN.slax
set groups juniper-ais system scripts op file ais-rsi-chk.slax
set groups juniper-ais system scripts op file ais-param-set.slax
set groups juniper-ais system scripts op file ais-sleep.slax
set groups juniper-ais system scripts op file ais-error.slax
set groups juniper-ais system scripts op file ais-health-report.slax
set groups juniper-ais system scripts op file ais_xfer_jmb.slax
set groups juniper-ais system scripts op file ais_policy_create.slax
set groups juniper-ais event-options event-script max-datasize 128m
set groups juniper-ais event-options event-script file intelligence-event-main.slax
set groups juniper-ais event-options event-script file bios.slax
set groups juniper-ais event-options event-script file phdc.slax
set groups juniper-ais event-options event-script file Master-event-struct.slax
set groups juniper-ais event-options event-script file Master-event-unstruct.slax
set groups juniper-ais event-options event-script file Master-policy-events.slax
set groups juniper-ais event-options event-script file User-event-struct.slax
set groups juniper-ais event-options event-script file User-event-unstruct.slax
```

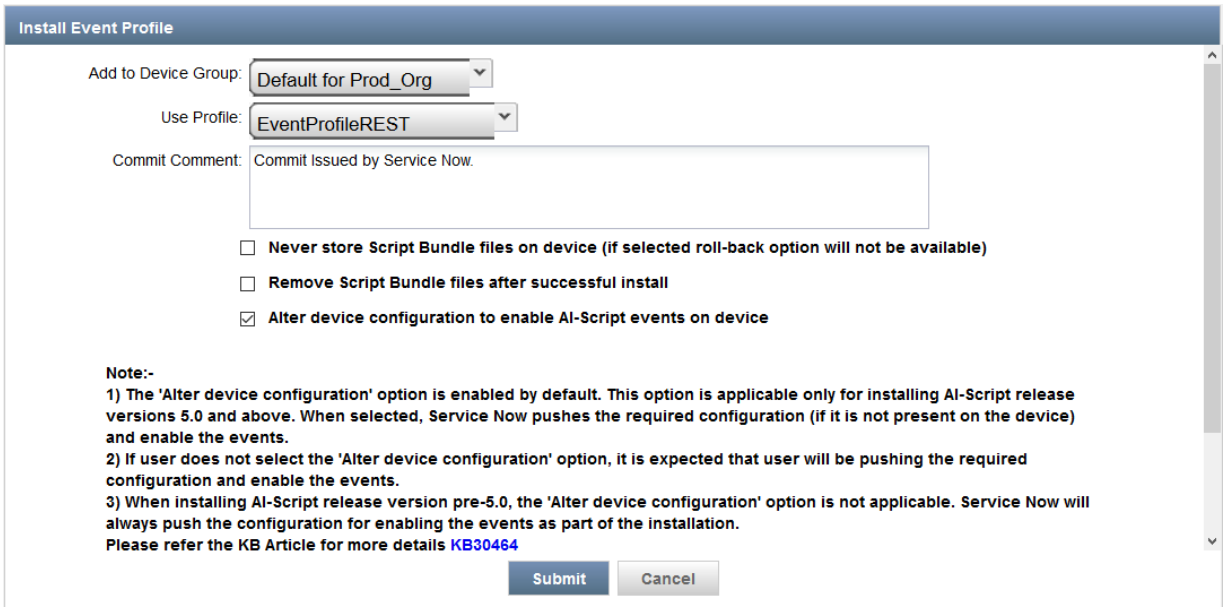
```
set groups juniper-ais event-options event-script file User-policy-events.slax
set groups juniper-ais event-options event-script file jais-scripts-add.slax
set groups juniper-ais event-options destinations juniper-aim archive-sites /var/tmp
set apply-groups juniper-ais
```

Service Now provides the following options to install and uninstall AI-Scripts on the managed devices without modifying the device configuration:

- The **Alter device configuration to enable AI-Script events on device** check box on the Install Event Profiles page (as shown in Figure 33 on page 206) provides the option to install AI-Scripts on a managed device without modifying the device configuration.

  This check box is selected by default. To avoid the device configuration from being modified when you install or upgrade and subsequently commit AI-Scripts, clear this check box.

Figure 33: Install Event Profile Page



NOTE:

- If you clear the **Alter device configuration to enable AI-Script events on device** check box and the static AI-Scripts configuration is not present on the device, Service Now only installs the AI-Scripts bundle on the device.

  For AI-Scripts to be configured and JMBs generated on the device, you must manually push the static AI-Scripts configuration and execute the **/var/db/scripts/op/ais-param-set.slax** file on the device.

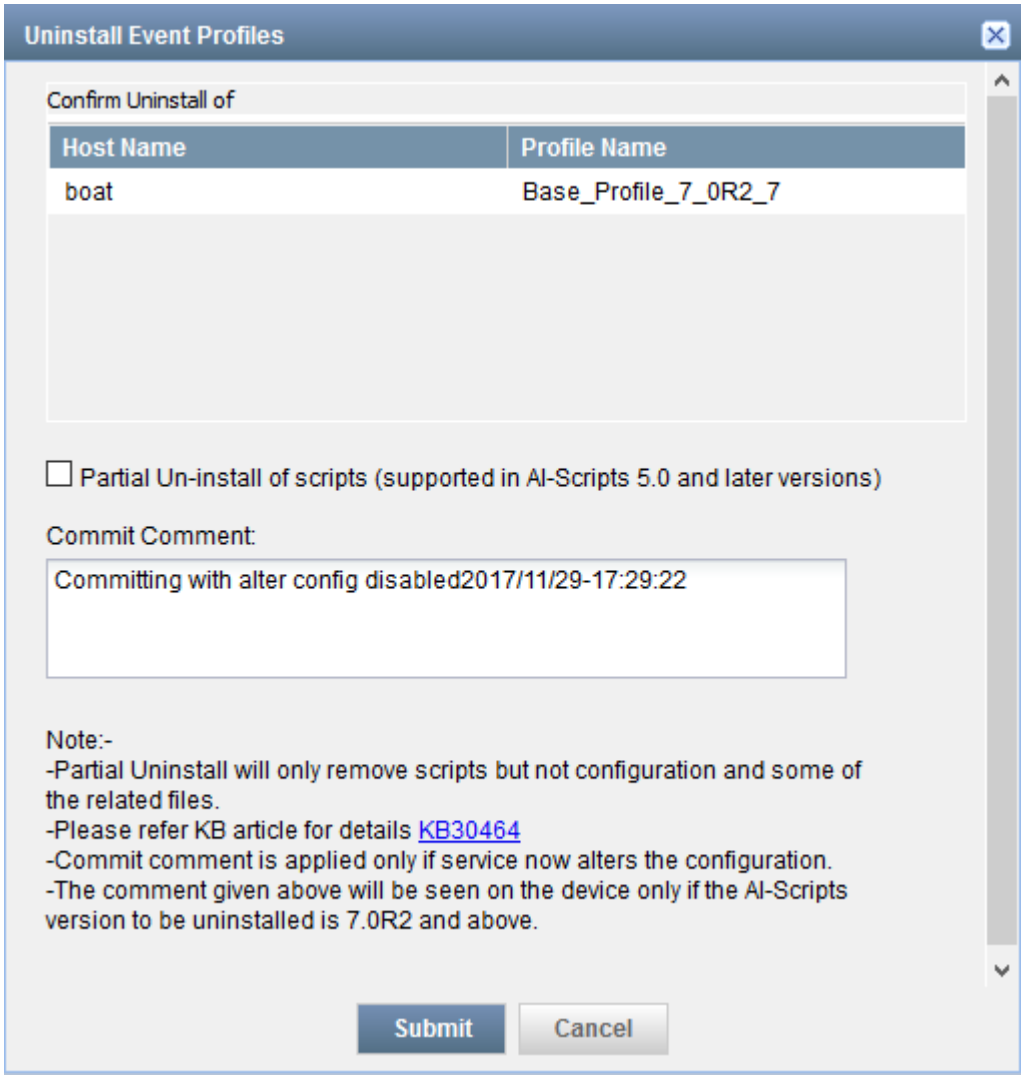
- When you install or upgrade AI scripts releases earlier than Release 5.0 on a device by using Service Now Release 15.1 or later, you must manually push the static AI-Scripts configuration to the device for each installation and upgrade irrespective of whether the Alter device configuration to enable AI-Script events on device check box is selected or cleared.

For information about installing AI-Scripts on a device, see "Installing an Event Profile on a Device by Using Service Now" on page 156.

- The **Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)** check box on the Uninstall Event Profiles dialog box, as shown in Figure 34 on page 208, when selected, provides an option to uninstall AI-Scripts from a device without modifying the device configuration.

  This option is cleared by default. When you uninstall AI-Scripts with this option selected, subsequent installation or upgrade of AI-Scripts does not modify the device configuration.

Figure 34: Uninstall Event Profile Dialog Box



NOTE: If you uninstall AI-Scripts Release 5.0 or later with the **Partial Un-Install of scripts(Supported in AI-Script 5.0 and above versions)** option cleared, you must delete the AI-Scripts configuration on the device by executing the **/var/db/scripts/remove-jais.slax** script on the device to avoid errors while committing the AI-Scripts configuration during the next installation or upgrade.

For information about uninstalling AI-Scripts from a device, see "Uninstalling an Event Profile from a Device" on page 165.

Associated Actions

You can perform the following actions related to event profiles:

- Add an event profile to Service Now; see "Adding an Event Profile to Junos Space Service Now" on page 210 for details.
- Push an event profile to devices; see "Installing an Event Profile on a Device by Using Service Now" on page 156 for details.
- View devices associated with an event profile; see "Displaying Devices Associated with an Event Profile" on page 229 for details.
- Set an event profile as default; see "Setting an Event Profile as the Default Event Profile in Junos Space Service Now" on page 225 for details.
- Import an event profile in XML format; see "Importing Event Profiles into Junos Space Service Now in XML Format" on page 219 for details.
- Export events data to Excel format; see "Exporting Events Data in Excel Format" on page 229 for details.
- Export an event profile in XML format; see "Exporting Event Profiles from Junos Space Service Now in XML Format" on page 230.
- Clone an event profile; see "Cloning an Event Profile" on page 214 for details.
- Delete event profiles; see "Deleting Event Profiles from Junos Space Service Now" on page 221 for details.
- Add script bundles; see "Adding a Script Bundle to Junos Space Service Now" on page 226 for details .

Release History Table

Release	Description
15.1R1	Starting in Service Now Release 15.1R1, when AI-Scripts Release 5.0R1 is installed (or an earlier version is upgraded to Release 5.0R1) on the device for the first time, a static AI-Scripts configuration is pushed and commited on the device. The static configuration, once committed on the device, is used during successive installation or upgrade of AI-Scripts. This eliminates the need for pushing and committing AI-Scripts configuration for each AI-Scripts installation or upgrade.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Service Now Devices Overview | 147

Service Now Incidents Overview

Adding an Event Profile to Junos Space Service Now

An event profile is a set of scripts that are selected from an AI-Scripts bundle. By 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 and use another AI-Scripts bundle (see "Adding a Script Bundle to Junos Space Service Now" on page 226).

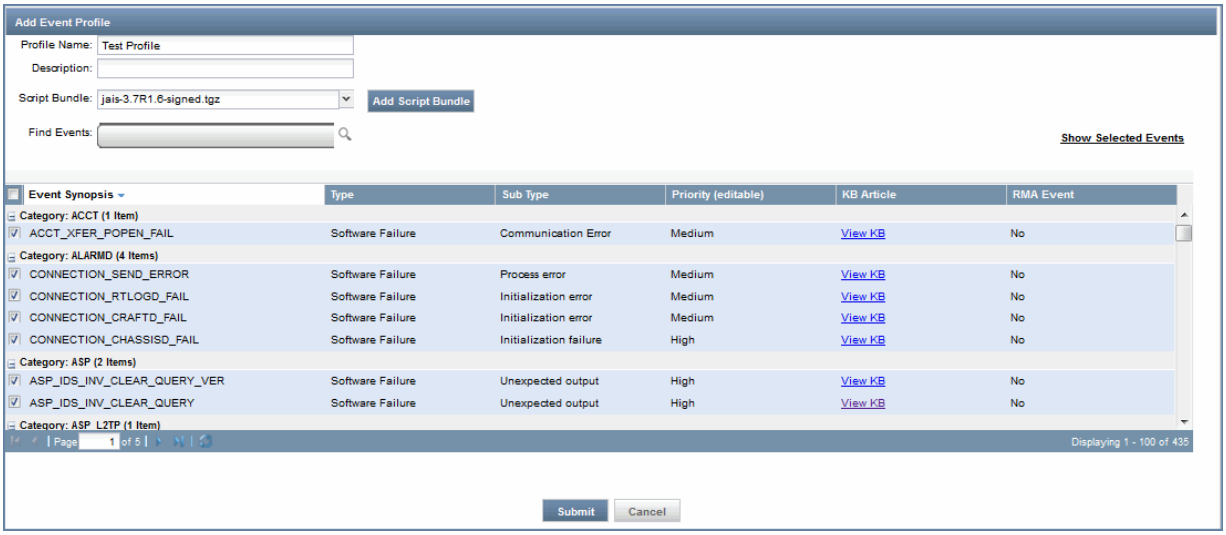
After you add an AI-Scripts bundle to Service Now, to be able to install the AI-Scripts bundle on the devices, you must create an event profile using this AI-Scripts bundle.

To add an event profile:

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

   The Add Event Profile page appears as shown in Figure 35 on page 210.

Figure 35: Add Event Profile Page



For a description of the fields displayed on this page, see Table 20 on page 210.

Table 20: Add Event Profile Page Field Descriptions

Field	Description
Profile Name	Enter a name of the event profile. The name can contain alphanumeric characters, underscore, hyphens and space. The maximum number of characters allowed is 255.

Table 20: Add Event Profile Page Field Descriptions *(continued)*

Field	Description
Description	Enter a description for the event profile. The maximum number of characters allowed is 255.
Script Bundle	Lists the 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	Specify an event from the list to filter the displayed list of events
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: • Hardware failure • Software failure • Resource Exhaustion
Sub Type	A brief description of the event type that triggers the event script to execute. 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.
Priority	Priority level of the event script. The values are: 1. Low 2. Medium 3. High 4. Critical
KB Article	Provides a link to knowledge base where you can find information such as cause and solution for the event..
RMA Event	Specifies if this is an RMA event or not.

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. If you want to add a new script bundle and use the new script bundle to create an event profile, click **Add Script Bundle**. See "Adding a Script Bundle to Junos Space Service Now" on page 226 for details about adding a new script bundle to Service Now.

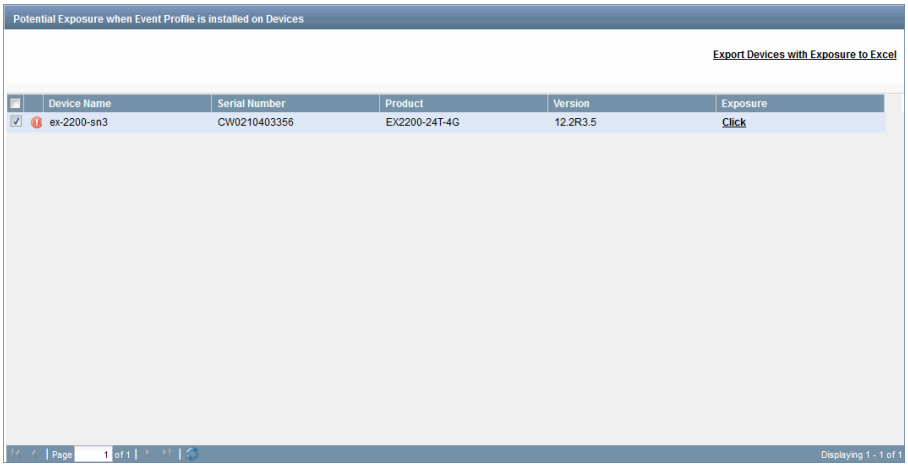
   By default, the script bundle that is set as the default is automatically selected for installing the event profile. You can modify this selection if required.

6. (Optional) To search for specific events to be included in the event profile, use the **Find Events** field.

7. Click **Submit**.

   An event profile is created with your specifications and the Save Event Profile dialog box appears.

8. On the Save Event Profile dialog box, 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. An icon (!) appears on the left-side of the row of a device on which the selected events in the event profile are likely to occur. **Figure 36: 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. 3. Click **Return to Potential Exposure** to continue. 4. Click **Continue**. A confirmation dialog box appears displaying the final list of devices on which you want to install the selected event profile. You can remove devices from the list by clearing the check boxes of the devices you want to remove . 5. Click **Install**. The event profile is installed on the selected devices, and the Service Now Devices page appears.
Apply this profile to devices manually	The Push to Devices page appears. Here you can select Service Now devices on which you want to install the event profile. For more information, see "Pushing an Event Profile to Devices" on page 221 .
Return to the Profiles Page	The event profile installation task is canceled, and the Event Profiles page appears.

RELATED DOCUMENTATION

Installing an Event Profile on a Device by Using Service Now | 156

Service Now Event Profiles Overview | 203

Cloning an Event Profile

Junos Space Service Now provides the Clone option in the Actions list of the Event Profiles page to clone an existing event profile and modify its priority to create another event profile. When you clone an event profile, Service Now provides a default name by appending the name of the original event profile with *Copy of*. You can edit this name.

> **NOTE:** Editing an event profile is similar to cloning an event profile. You cannot edit an event profile.

To clone an event profile:

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

2. Select the event profile that you want to clone, and select **Clone** from either the **Actions** list or the right-click menu.

   The **Clone Event Profile** page appears.

3. (Optional) In the **Profile Name**, edit the profile name.

   By default, Service Now populates the name of the event profile as a Copy of *event profile* from which the new event profile is being cloned.

4. (Optional) In the **Description** text field, enter a description for the cloned event profile.

5. (Optional) From the **Script Bundle** list, select a script bundle from which to create the cloned event profile..

   A **Show difference** button appears.

6. (Optional) Click the **Show difference** button to view the differences in the events between the original script bundle and the newly selected script bundle.

The Event Difference Display dialog box displays the events that are new and deprecated in the newly selected script bundle in comparison with the script bundle used in the original event profile.

After viewing the differences, close the Event difference display dialog box to return to the Clone Event Profile page.

7. (Optional) To search for specific events, enter the name of the event in the **Find Events** search field.

8. (Optional) Click **Priority** for each event to modify the event priority. The values are:

    1. Low
    2. Medium
    3. High
    4. Critical

9. Click **Submit**. The event profile is created and the **Save Event Profile** dialog box appears.

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

Link	Result
Apply this profile to original set of devices	

Link	Result
	When you click this link, the Select Devices to Install Profile section appears on the Clone Event Profile page.. In this page, specify the following options for installing the profile on the devices: • Specify the devices on which you want to install the event profiles by selecting the respective check box present on the left side of the row. To specify all the listed devices, select the check box present next to **Organization** column heading. • 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. This check box is cleared by default. **NOTE:** If you select this check box, roll back to this version of the AI-Scripts bundle is not possible in future. • 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.. • if you do not want the device configuration to be modified while committing the event profile on the device, clear the **Alter device configuration to enable AI-Script events on device** check box. By default, this option is selected. **NOTE:** ◦ If you clear the Alter device configuration to enable AI-Script events on device check box and the static AI-Scripts configuration is not present on the device, Service Now only installs the AI-Scripts bundle on the device. The static AI-Scripts configuration must be committed on the device manually and the **/var/db/scripts/op/ais-param-set.slax** file executed for AI-Scripts to generate JMBs. ◦ When you install or upgrade AI scripts releases earlier than Release 5.0 on a device using Service Now Release 15.1 or later, the static AI-Scripts configuration must be pushed manually to the device for each installation and upgrade irrespective of whether the Alter device configuration to enable AI-Script events on device check box is selected or cleared. • If you want to install the event profiles later on the devices, schedule the installation. Selecting the **Schedule at a later time** check box provides the controls to specify the date and time of the installation. Click **Submit** to proceed with the installation. The Potential Exposure when Event Profile is Installed on Devices page displays the selected set of devices. An (!) icon present on the left-side of a device row indicates that the device is susceptible to events in the event profile.

Link	Result
	On this page, you can • Export information on devices susceptible to events. To export device data in an Excel format, click **Export Devices with Exposure to Excel**. • View the events to which a device is susceptible. To view the events to which a device is susceptible, 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. To proceed with the installation: 1. Select the devices on which you want install the event profile and click **Continue**. The Install Event Profile dialog box appears. 2. Click **Install** or **Cancel** to confirm or cancel the installation of the event profiles on the selected devices.
Apply this profile to devices manually	When you click this link, the Push to Devices page appears. On this page, you can select Service Now devices and install event profiles on the selected devices. For information about installing event profiles on devices, see "Pushing an Event Profile to Devices" on page 221.
Return to the Profiles Page	When you click this link, Service Now cancels the installation of event profile on devices and displays the Event Profiles page. The cloned event profile is listed on the Event Profiles page.

RELATED DOCUMENTATION

Installing an Event Profile on a Device by Using Service Now | 156

Service Now Event Profiles Overview | 203

Importing Event Profiles into Junos Space Service Now in XML Format

Junos Space Service Now provides the Import Event Profiles option in the Actions list of the Event Profiles page to import event profiles in the XML format to Service Now. You can import only one XML file at a time. To import multiple event profiles at the same time, include all the event profiles in the same XML file. Each event profile that is imported is listed on the Event Profiles page.

The following is a sample of the XML file containing event profiles for importing into Service Now:

```
<eventProfiles>
  <eventProfile>
       <profileInformation>
       <profileName>Base_profile</profileName>
       <description>Base Profile for Bundle 4.1R1.1</description>
       <scriptBundleVersion>6.0R1.0</ scriptBundleVersion >
       <scriptBundleFileName>jais-6.0R1-signed.tar</scriptBundleFileName>
       <creationTime>[In seconds]</creationTime>
       <userCreated>super<userCreated>
       <eventsIncluded>440</eventsIncluded>
       <eventsExcluded>0<eventsExcluded>
       <deviceInstalled>2</deviceInstalled>
     </profileInformation>

     <scripts>
       <script>
      <scriptId>47</scriptId>
           <eventId>ACCT_MALLOC_FAILURE</eventId>
         <scriptName>ACCT_MALLOC_FAILURE.slax</scriptName>
             <processId>PFED</processId>
           <eventTypeGroup>Resource Exhaustion<eventTypeGroup>
           <eventType>Memory Consumption</eventType>
          <priority>3</priority>
          <userDescription>ACCT_MALLOC_FAILURE</userDescription>
         <eventDescription>The accounting statistics process could not allocate
memory from the heap.</eventDescription>
         <activateDescription>Capture ACCT_MALLOC_FAILURE
Events</activateDescription>
         <featureName>ACCT_MALLOC_FAILURE.slax</featureName>
         <minimumVersion>9.4</minimumVersion>
         <helpText>ACCT_MALLOC_FAILURE</helpText>
         <expressRMA>FALSE</expressRMA>
```

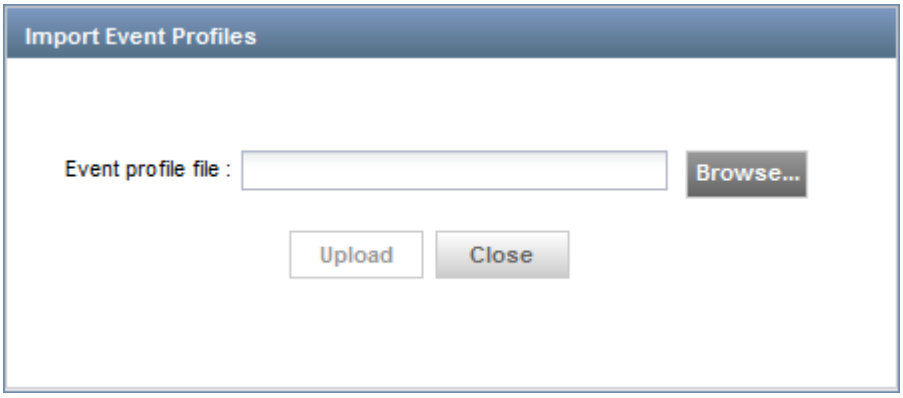
```
        <kbUrl>KB18749</kbUrl>
        <platformList>
          <platform>PFE_CHIPSET_ABSENT</platform>
        </platformList>
     </script>
 ...
 ...
 ...

   </scripts>
</eventProfile>
<eventProfile>
...
...
...
</eventProfile>
</eventProfiles>
```

To Import event profiles into Service Now in the XML format:

1. On the Service Now navigation tree, select **Administration > Event Profiles > Import Event Profiles**.

   The Import Event Profiles page appears as shown in Figure 37 on page 220.

Figure 37: View Event Profiles Page



2. Click **Browse** to browse for the event profile file and click **Upload**.

   Service Now imports the event profile file and lists the imported event profiles on the Event Profiles page.

RELATED DOCUMENTATION

Service Now Event Profiles Overview | 203

Deleting Event Profiles from Junos Space Service Now

Junos Space Service Now provides the Delete option in the Actions list of the Event Profiles page to delete event profiles. You can delete an event profile only if it is not associated with a device.

When you delete a default event profile, Service Now sets the most recently created event profile as the default event profile.

To delete event profiles:

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

   The Event Profiles page appears.

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

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

3. Click **Delete** to confirm.
   Service Now deletes the selected event profiles and removes the deleted event profiles from the Event Profiles page.

RELATED DOCUMENTATION

Displaying Devices Associated with an Event Profile | 229

Pushing an Event Profile to Devices

An event profile is a set of event policies that are selected from an AI-Scripts bundle. When you push an event profile onto Juniper Networks devices, these event policies are installed on the devices. The event policies automatically detect and report problems (incident) that occur on the device and also provide monitoring information.

Junos Space 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 install event profiles on the devices of end customers.
- For information about behavior of AI-Scripts when installed on specific product families, see https://kb.juniper.net/InfoCenter/index?page=content&id=KB29188.

To install an event profile on devices:

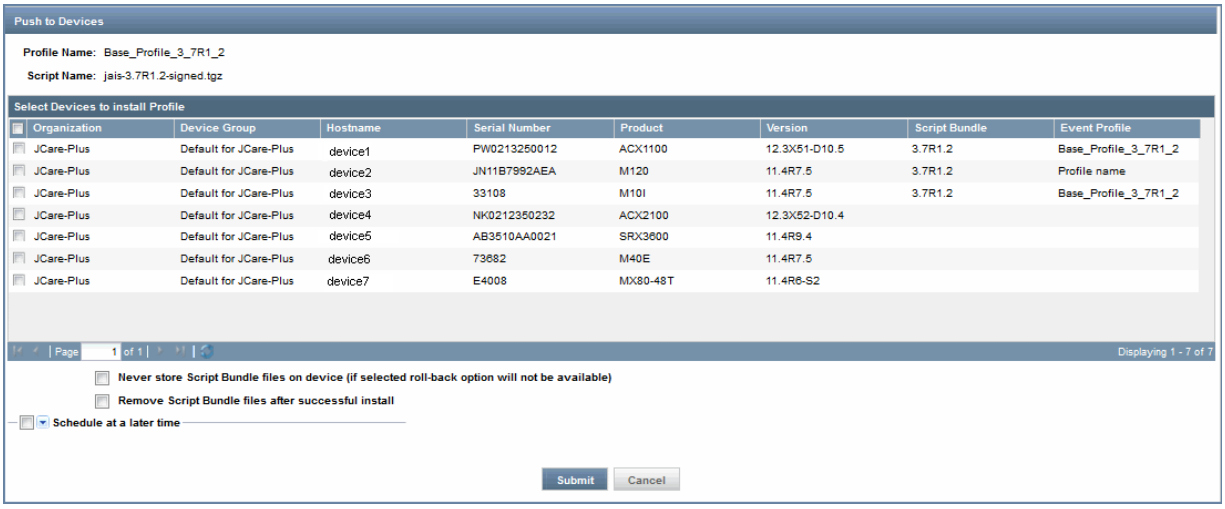
1. From the Service Now taskbar, select **Administration** > **Event Profiles**.

   The 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** list or the right-click menu.

   The **Push to Devices** page appears (see Figure 38 on page 222).

Figure 38: Push to Devices Dialog Box



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. Under the Select Devices to Install Profile section, 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 do not want the device configuration to be modified while committing the event profile on the device, clear the **Alter device configuration to enable AI-Script events on device** check box.

   By default, this option is selected.

   NOTE:
   - If you clear the Alter device configuration to enable AI-Script events on device check box and the static AI-Scripts configuration is not present on the device, Service Now only installs the AI-Scripts bundle on the device. The static AI-Scripts configuration must be committed on the device manually and the **/var/db/scripts/op/ais-param-set.slax** file executed for AI-Scripts to generate JMBs.
   - When you install or upgrade AI scripts releases earlier than Release 5.0 on a device using Service Now Release 15.1 or later, the static AI-Scripts configuration must be pushed manually to the device for each installation and upgrade irrespective of whether the Alter device configuration to enable AI-Script events on device check box is selected or cleared.

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 when you want to install the event profile in the **Date and time** field.

   Service Now installs the event profile at the configured date and time.

8. Click **Submit**.

   The Potential Exposure when Event Profile is Installed on Devices page appears and displays information about the selected set of devices. An icon (!) appears on the left side of the rows of devices that are susceptible to the events in the event profile.

Figure 39: Potential Exposure to Known Issues Page

9. (Optional) To export device data in an Excel format, click **Export Devices with Exposure to Excel**.

10. (Optional) To view the events to which the device is susceptible, click the respective link displayed in the **Exposure** column.

    The View Exposure page appears and displays the known issues associated for the respective device.

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

12. To proceed with the installation, Click **Continue**.

    The Install Event Profile dialog box appears. You can remove devices from the list by clearing their respective check boxes.

13. 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 Jobs page displays the status of the job. The **Device Details** dialog box also displays the status of script installation on the selected devices.

If you have installed the event profile on a dual Routing Engine, the results displayed on the Jobs page shows the status for both the primary Routing Engine and the backup Routing Engine. A **Failed** status indicates that the installation failed on either of the Routing Engines.

14. Click **OK**.

    The View Event Profiles page appears.

RELATED DOCUMENTATION

Service Now Event Profiles Overview | 203

Viewing Exposure for a Device | 196

Setting an Event Profile as the Default Event Profile in Junos Space Service Now

Junos Space Service Now provides the Set as Default Profile option in the Actions list of the Event Profiles page 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 Event Profiles page. If you delete the default event profile, the latest event profile created is automatically set as the default.

To set an event profile as the default:

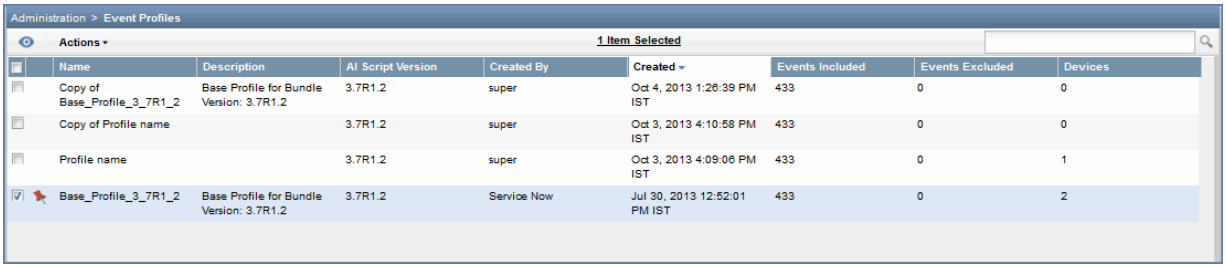
1. From the Service Now taskbar, select **Administration** > **Event Profiles**.
   The Event Profiles page appears.

2. Select the event profile that you want to set as the default, and select **Set as Default Profile** from either the **Actions** list or the right-click menu.

   The **Set As Default Profile** dialog box appears and prompts you for 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 in the Service Now Devices page for installing an event profile. The default event profile (for example, Base_Profile_3_7R1_2 in Figure 40 on page 226) shows the default event profile indicated by the unique icon.

Figure 40: View Event Profiles Page



RELATED DOCUMENTATION

Displaying Devices Associated with an Event Profile | 229

Cloning an Event Profile | 214

Pushing an Event Profile to Devices | 221

Adding a Script Bundle to Junos Space Service Now

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

NOTE: The script bundle is distributed as a ***.tgz** file for releases prior to AI-Scripts Release 6.0R1.0. From AI-Scripts Release 6.0R1.0, the script bundle is distributed as a ***.tar** file.

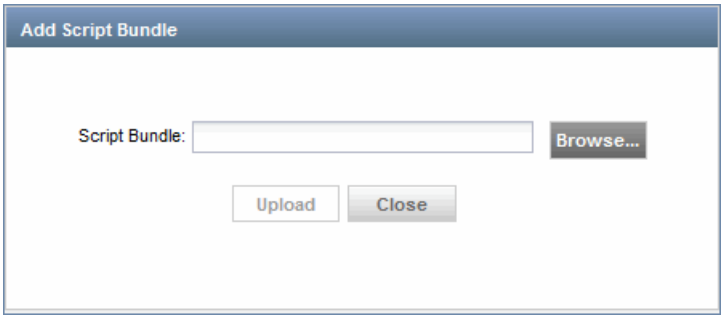
After you add a script bundle to Service Now, to be able to install the script bundle on devices, you must first create an event profile by using this script bundle. See “Adding an Event Profile to Junos Space Service Now” on page 210.

To add a script bundle:

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

   The Add Script Bundle page appears as shown in Figure 41 on page 227.

Figure 41: 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 to Service Now and appears on the Script Bundles page.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Installing an Event Profile on a Device by Using Service Now | 156

Setting a Script Bundle as the Default Script Bundle in Junos Space Service Now

Junos Space Service Now provides the Set as Default Bundle option in the Actions list of the Script Bundles page 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 policies to be included in the event profile. The default script bundle is represented by a unique icon on the Script Bundles page. If you delete the default script bundle, Service Now sets the most recently uploaded script bundle as the default script bundle.

To set a script bundle as the default:

1. From the Service Now navigation tree, select **Administration** > **Script Bundles**.

   The 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** list 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 Script Bundles page.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Installing an Event Profile on a Device by Using Service Now | 156

Deleting a Script Bundle from Junos Space Service Now

Junos Space Service Now provides the Delete option in the Actions list on the Script Bundles page to delete script bundles.

You cannot delete a script bundle if:

- The script bundle is preloaded with Service Now
- An event profile created by using the script bundle is installed on a device

To delete a script bundle:

1. From the Service Now navigation tree, select **Administration** > **Event Profiles** > **Script Bundles**.

   The Script Bundles page lists the available script bundles.

2. Select the script bundles that you want to delete, and select **Delete Script Bundles** from either the **Actions** list or the right-click menu.

   The Delete AI-Scripts dialog box appears and prompts you to confirm the deletion.

3. Click **Delete**.

   Service Now deletes the script bundles from the database and returns to the Script Bundles page. The deleted script bundles are no longer listed on the Script Bundles page.

RELATED DOCUMENTATION

AI-Scripts Overview | 21

Installing an Event Profile on a Device by Using Service Now | 156

Displaying Devices Associated with an Event Profile

Junos Space Service Now provides the Show Associated Devices option in the Actions list of the Event Profiles page to view devices that are associated with a specific event profile. This task is disabled when you select an event profile that is not associated with any device.

To display devices associated to an event profile:

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

   The 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** list or the right-click menu.

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

RELATED DOCUMENTATION

Installing an Event Profile on a Device by Using Service Now | 156

Adding an Event Profile to Junos Space Service Now | 210

Exporting Events Data in Excel Format

Junos Space Service Now enables you to export data such as the number of times a particular event occurred in the devices in the last 7 days, 30 days, 365 days, events that never occurred, and the day on which new events occurred to an Excel file and save it on your local file system.

To export events data to an Excel file:

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

2. Double-click the event profile whose event activity you want to export.

   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 browser dialog box allows you to open or save the Excel file.

4. Select **Open with** to open the Excel file or select **Save File** to save the file on your local system.

5. Click **OK**.
   The event activity information that appears in the Event Profile Detail dialog box is contained in the following five worksheets in the Excel file:

   - Event Activity(7 days)
   - Event Activity(30 days)
   - Event Activity(365 days)
   - New Active Events
   - Inactive Selected Events

RELATED DOCUMENTATION

Installing an Event Profile on a Device by Using Service Now | 156

Service Now Event Profiles Overview | 203

Exporting Event Profiles from Junos Space Service Now in XML Format

Junos Space Service Now provides the Export All Profiles and Export Selected Profiles options on the Actions list of the Event Profiles page to export event profiles in the XML format. Service Now includes all event profiles to be exported in a single XML file.

The following sample is an example of an event profile exported by Service Now:

```
<eventProfiles>
  <eventProfile>
       <profileInformation>
       <profileName>Base_profile</profileName>
       <description>Base Profile for Bundle 4.1R1.1</description>
       <scriptBundleVersion>6.0RR1.1</ scriptBundleVersion >
       <scriptBundleFileName>jais-6.0R1-signed.tar</scriptBundleFileName>
       <creationTime>[In seconds]</creationTime>
       <userCreated>super<userCreated>
       <eventsIncluded>440</eventsIncluded>
       <eventsExcluded>0<eventsExcluded>
       <deviceInstalled>2</deviceInstalled>
     </profileInformation>

     <scripts>
       <script>
      <scriptId>47</scriptId>
           <eventId>ACCT_MALLOC_FAILURE</eventId>
         <scriptName>ACCT_MALLOC_FAILURE.slax</scriptName>
             <processId>PFED</processId>
            <eventTypeGroup>Resource Exhaustion<eventTypeGroup>
            <eventType>Memory Consumption</eventType>
          <priority>3</priority>
          <userDescription>ACCT_MALLOC_FAILURE</userDescription>
          <eventDescription>The accounting statistics process could not allocate
memory from the heap.</eventDescription>
         <activateDescription>Capture ACCT_MALLOC_FAILURE
Events</activateDescription>
         <featureName>ACCT_MALLOC_FAILURE.slax</featureName>
         <minimumVersion>9.4</minimumVersion>
         <helpText>ACCT_MALLOC_FAILURE</helpText>
         <expressRMA>FALSE</expressRMA>
         <kbUrl>KB18749</kbUrl>
         <platformList>
           <platform>PFE_CHIPSET_ABSENT</platform>
         </platformList>
     </script>
 ...
 ...
 ...

   </scripts>
</eventProfile>
```

```
</eventProfiles>
```

To export event profiles in the XML format:

1. In the Service Now navigation tree, select **Administration > Event Profiles**.

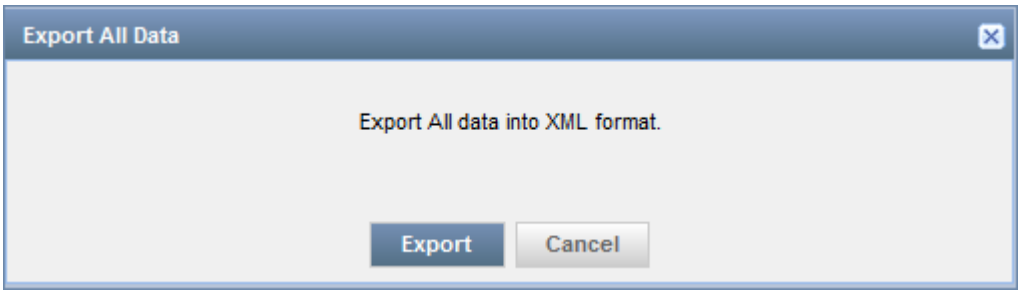
   The Event Profiles page appears.

2. On the Event Profiles page, do one of the following:

   - To export all event profiles from Service Now, select **Export All Profiles** from the Actions list. Alternatively, right-click on an event profile and select **Export All Profiles**.

     The Export All Data dialog box appears as shown in Figure 42 on page 232.

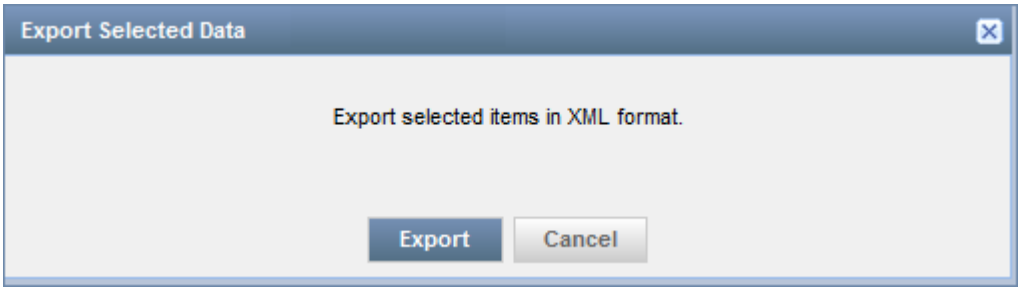
Figure 42: Export All Data Dialog Box



   - To export selected event profiles, click the event profiles that you want to export and select **Export Selected Profiles** from the Actions list. Alternatively, you can click the event profiles that you want to export and select **Export Selected Profiles** from the right-click menu.

     The Export All Data dialog box appears as shown in Figure 43 on page 232.

Figure 43: Export All Data Dialog Box



3. Click **Export**.

The Export Job Status dialog box appears. A **Download** link appears on the dialog box to download the XML file after the export job is complete.

4. Click the **Download** link to view or save the XML file on your local system.

RELATED DOCUMENTATION

Service Now Event Profiles Overview | **203**

Importing Event Profiles into Junos Space Service Now in XML Format | **219**

11

CHAPTER

Configuring and Managing Auto Submit Policies

Service Now Auto Submit Policy Overview | **237**

Creating an Auto Submit Policy | **239**

Modifying an Auto Submit Policy | **245**

Changing the Status of Auto Submit Policies | **247**

Deleting Auto Submit Policies from Service Now | **248**

Exporting an Incidents Report | **249**

Changing the Dampening Status of an Auto Submit Policy | **250**

Service Now Auto Submit Policy Overview

An auto submit policy allows Service Now to submit incidents to Juniper Support Systems or a Service Now partner (JSS) automatically. When Service Now submits an incident to JSS, JSS creates a technical support case and provides the case ID to Service Now. After a case is created in JSS, Service Now updates the status of the incident as Case Created along with the case number.

An auto submit policy lets you configure Service Now to prevent creating incidents when a JMB is received for the same event within a configured time interval. This is called dampening. Dampening policy is assigned to individual events if the Auto Submit Policy is activated. You can select a dampening period for which alerts are dampened for an event that recurs on the same device, device group, or organization.

Service Now displays the configured auto submit policies on the Auto Submit Policy page (**Administration** > **Auto Submit Policy**).

Service Now uses the event ID and synopsis of an event to dampen incident creation. Whenever an event occurs on a device, Service Now checks if an auto submit policy is defined for that event. If an auto submit policy is defined, Service Now checks for the dampening status on the policy. If the dampening status is enabled, Service Now gets the user-defined dampening interval for the event reported on a device. If a dampening interval is found, Service Now checks when the last incident was created for the event ID and synopsis. If the last event occurred before the defined dampening interval or if it had occurred during the defined dampening interval but the incident for the last event is in the closed state, Service Now creates a new incident for the event; otherwise, Service Now does not create an incident. Event RMA is always dampened.

To view auto submit policies, select **Administration** > **Auto Submit Policy**, from the Service Now taskbar. The Auto Submit Policy page appears as shown in Figure 44 on page 237.

Figure 44: Auto Submit Policy Page

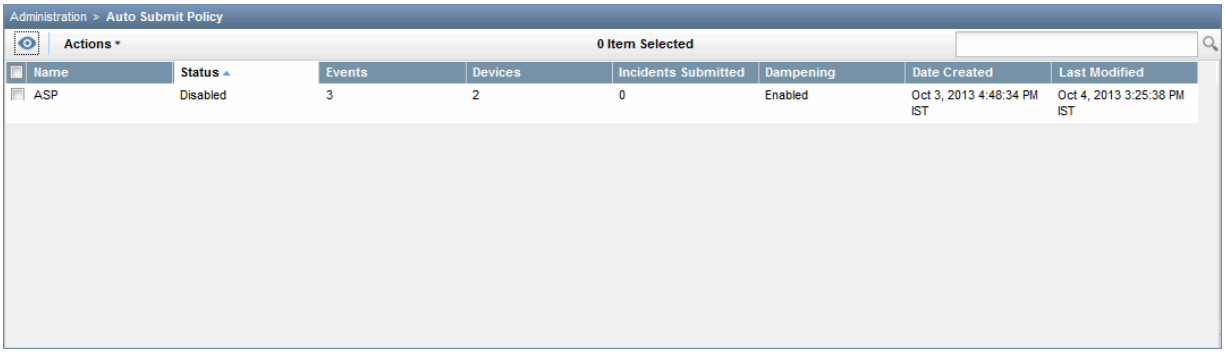


Table 21 on page 238 lists the parameters of an auto submit policy.

Table 21: Auto Submit Policy Parameters

Parameter	Description
Name	Name of the auto submit policy.
Status	Status of the auto submit policy. Possible values: • Enabled—The auto submit policy can be applied to devices for automatically submitting incidents for creating cases. • Disabled—The auto submit policy cannot be applied to devices for automatically submitting incidents for creating cases.
Events Count	Number of events included in the event profile.
Devices Count	Number of devices to which the auto submit policy is assigned.
Filters Count	Number of filters associated with the auto submit policy.
Incidents Submitted	Number of incidents submitted for creating case by using the auto submit policy.
Dampening	Indicates whether incident creation should be dampened for the events included in the auto submit policy. **NOTE:** The dampening status for individual events override the dampening status of the auto submit policy.
Created By	User who created the auto submit policy.
Created Date	Date and time the auto submit policy was created.
Last Modified	Date and time the auto submit policy was last modified.
Devices	Devices to which the auto submit policy is assigned.
Filters	Auto submit filters associated with the auto submit policy.
Events	Events included in the auto submit policy.

Associated Actions

You can perform the following actions related to auto submit policies:

- Change the status of one or more auto submit policies; see "Changing the Status of Auto Submit Policies" on page 247 for details.
- Export details about the incidents created by using an auto submit policy; see "Exporting an Incidents Report" on page 249 for details.
- Delete auto submit policies; see "Deleting Auto Submit Policies from Service Now" on page 248 for details.
- Modify an auto submit policy; see "Modifying an Auto Submit Policy" on page 245 for details.
- Change dampening status; see "Changing the Dampening Status of an Auto Submit Policy" on page 250 for details.
- Assign an auto submit policy to another domain; see "Assigning a Service Now Object to Another Domain" on page 56 for details.

RELATED DOCUMENTATION

Creating and Editing a Notification Policy

Service Now Devices Overview | **147**

Service Now Auto Submit Filters Overview | **275**

Service Now Suppressed Events Overview

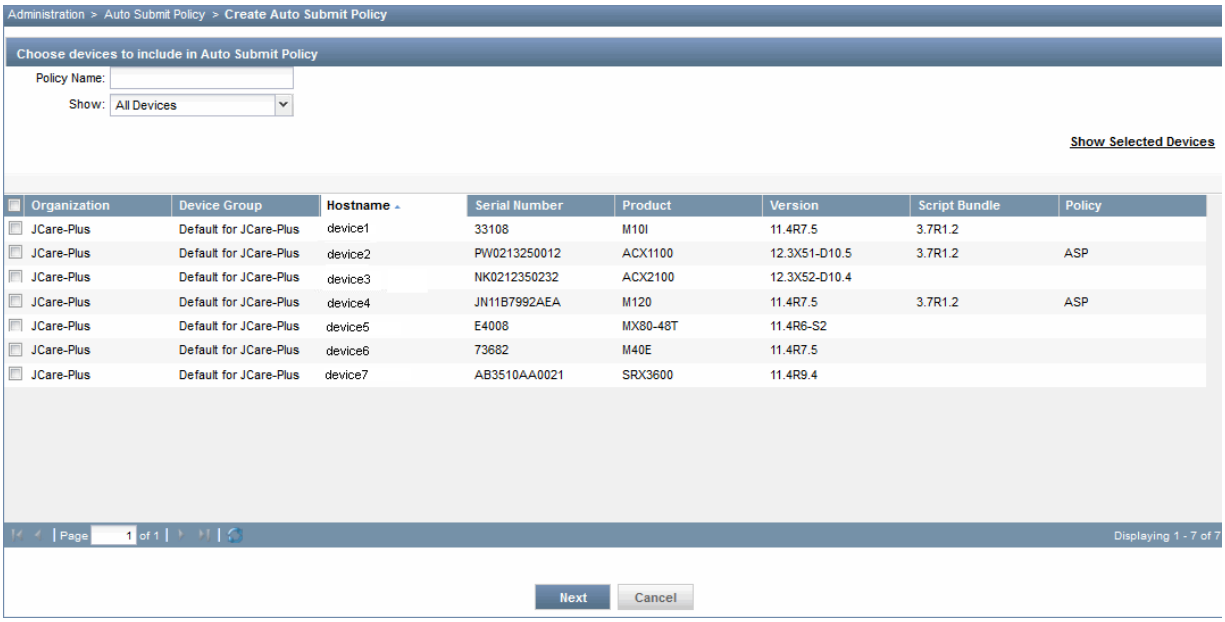
Creating an Auto Submit Policy

An auto submit policy enables Service Now to automatically submit incidents to JSS for creating a Tech Support Case. Although events with priority P1 can be included in an auto submit policy, Service Now does not submit incidents created for P1 events to JSS automatically.y Therefore, incidents created for P1 events must be submitted manually and JTAC should be called immediately.

To create an auto submit policy:

1. From the Service Now navigation tree, select **Administration** > **Auto Submit Policy** > **Create Auto Submit Policy**.
   The Choose devices to include in Auto Submit Policy page appears as shown in Figure 45 on page 240.

Figure 45: Auto Submit Policy Creation Page



2. In the **Policy Name** field, enter a name for the policy.

   The name can contain only alphanumeric (a-z, A-Z, 0-9), underscores (_), and hyphens (-). The maximum number of characters allowed is 255.

3. Select an option in the **Show** list as follows for assigning the auto submit policy to devices::

   - To filter devices by their organization, in the **Show** list, select **By Organization** and select an *Organization* in the **Organization** list.

     Service Now displays a list of devices belonging to the selected organization.

   - To filter devices by device group, in the **Show** list, select **By Device Group** and select a *Device Group* from the **Device Group** list.

     Service Now displays a list of devices belonging to the selected device group.

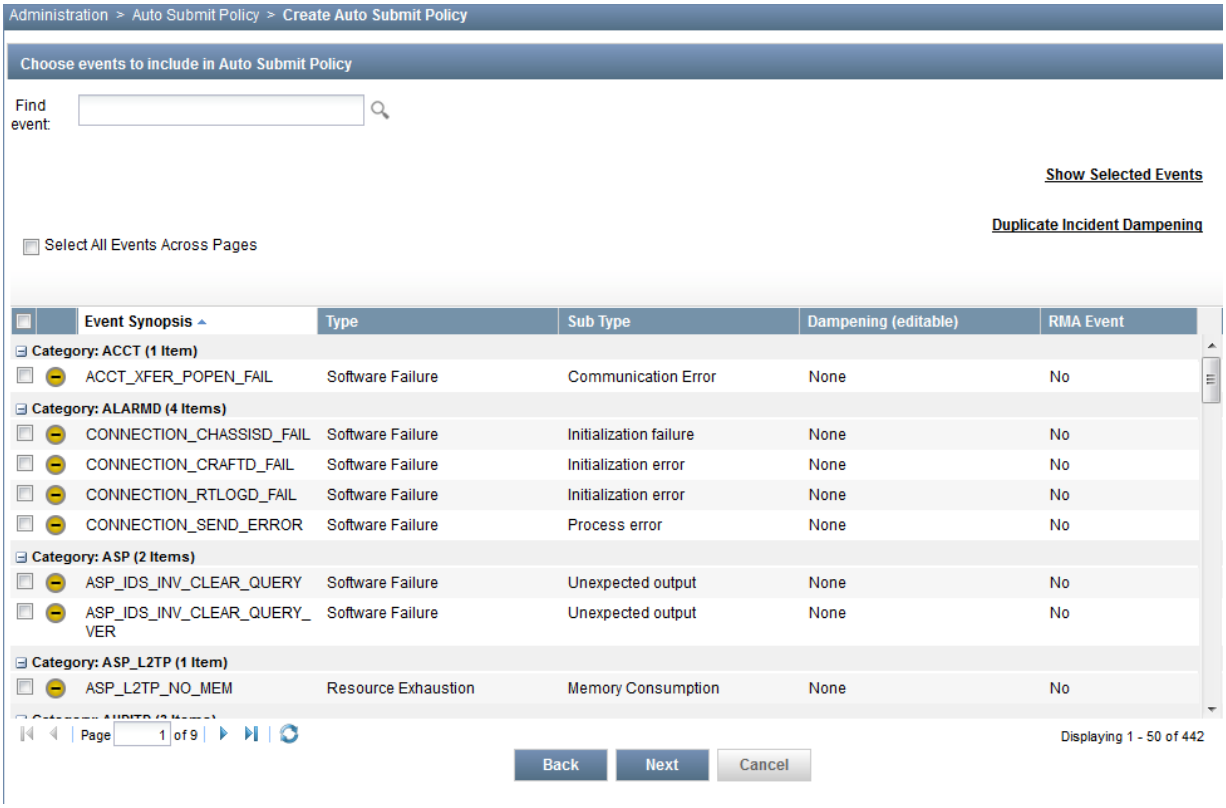
4. Select the devices for which you want to assign the auto submit policy.

5. (Optional) Click the **Show Selected Devices** link to view the list of devices selected for assigning the auto submit policy that you are creating.

The **Selected Devices** dialog box displays the list of devices that you selected. Verify the list and click **Close** to return to the previous page.

6. Click **Next**.
   The **Choose events to include in Auto Submit Policy** page appears.

Figure 46: Choose events to include in Auto Submit Policy Page



7. Select the events to be included in the auto submit policy by using one of the following options:
   - Select the **Select All Events Across Pages** check box to include all the listed events to the auto submit policy.
   - Manually select the events.

   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 22 on page 242).

> **TIP:** To find events, type the event name in the **Find event** search field and then select the event. As you type an event name, all the events with names beginning with the text that you entered are displayed in the list. For example, when you type **audi** in the **Find event** search field, all events with names beginning with audi are listed.

Table 22: Icons That Represent the Event Types and Their Descriptions

Event Icons	Descriptions
	Event is inactive for all the selected devices. Do not include this event in the auto submit policy.
	Event is inactive for some of the selected devices.
	Event is active for all the selected devices.
P1	Event is, by default, priority P1 for one or more selected devices. Although you can include these events in the auto submit policy, Service Now does not automatically submit these incidents for creating cases to JSS or Service Now partner. You can open a case for these events only by contacting JSS directly over phone.

8. (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.

9. Click the **Duplicate Incident Dampening** link to set the dampening interval for the selected events. The Duplicate Incident Dampening dialog box appears.

10. Select a dampening interval from the **Dampen Incidents for** drop-down list for each event as follows:

    - None: Select None to create an incident for each occurrence of the events on the selected devices.
    - Always: Select Always if you do not want an incident to be created after the first occurrence of the event on the selected devices. Service Now does not create another incident for the event until the first incident is closed or deleted.
    - Dampening intervals of 1hr, 2hr, 3hr, ...: Service Now does not create incidents for the specified time duration after the first occurrence of the event. However, if the first incident is closed or deleted within in the specified time duration, Service Now creates another incident for the same event.

11. Click **Next**.

The Choose filters to include in Auto Submit Policy page appears. This page lists the auto submit filters configured in Service Now and also provides the options to create basic and advanced auto submit filters, and reorder auto submit filters to change the order in which the filters are applied to incidents.

12. (Optional) Do one of the following tasks to assign auto submit filters to the auto submit policy:
    - Select one or more auto submit filters to be associated with the auto submit policy.
    - Click **Create Basic Filter** to create a basic auto submit filter and assign it to the auto submit policy.

      For information about creating basic auto submit filters, see "Creating a Basic Auto Submit Filter" on page 278.
    - Click **Create Advanced Filter** to create an advanced auto submit filter and assign it to the auto submit policy.

      For information about creating advanced auto submit filters, see "Creating an Advanced Auto Submit Filter" on page 280.
    - Click **Reorder Filters** to reorder the filters.

      The Reorder Filters page appears. Change the order of the filter by selecting the filter and clicking the up or down arrow to change the order.

      > **NOTE:** The order of filters in an auto submit policy is relevant to only that policy. The same filters can be associated with another policy and have a completely different order.

13. Click the **Next** button to proceed with creating the auto submit policy.

    The Submit Case Options page appears.

14. Click the **Enter Email Id** field to enter one or more e-mail IDs in the format user@example.com.

    Service Now sends notifications to the configured e-mail IDs when the incident is created and when the status of the incident changes.

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

15. (Optional) Click **Modify** to modify the site ID or username of the organization.

    The Make Selection to Change Site ID or Use dialog box appears.
    - To modify the site ID, click **Default Org**, and select the site ID from the **Site ID** list.
    - To modify the user name, click **User Name**, and enter the username and password of your organization in their respective fields. After your user credentials are validated, click **Get Sites** to select a site ID specific to the new user.

16. Click **OK**.
    The Summary of Auto Case Policy to be created page lists the details such as the selected events, the devices on which they occurred, the event synopsis, and the dampening status.

    The Submit Case Options page appears again.

17. (Optional) Select the **Upload Associated Core Files for Incident** check box to upload core files generated for the incident.

18. (Optional) Select the **Upload All Core Files** check box if you want the auto submit policy to upload all core files available on the device to the configured SFTP server for selected events.

19. (Optional) Select the **Delete Core Files from devices after uploading** check box If you want to delete core files from the device after uploading it to the SFTP server.

    You must select the **Delete Core Files from devices after uploading** in combination with the **Upload Associated Core Files for Incident** or **Upload All Core Files** check box.

    When you select the **Delete Core Files from devices after uploading** check box in combination with the **Upload Associated Core Files for Incident** check box, the core files associated with the event are deleted from the device after the core file is uploaded to Service Now.

    When you select the **Delete Core Files from devices after uploading** check box in combination with the **Upload All Core Files for Incident** check box, all core files present on the device are uploaded to Service Now and deleted from the device.

20. In the **Follow Up Method** list, select the method that you would like to use to follow up on the case associated with the incident—Email Full Text Update, Email Secure Web Link, or Phone Call.

21. In the **Priority** field, select the priority of the case.

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

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

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

23. In the **Add Comments to Synopsis** and **Add Comments to Description** fields, enter a synopsis and description for the incident.

    When submitting on-demand or off-box incidents, you can edit the auto-generated synopsis and description. The maximum number of characters allowed for the synopsis and description is 255 and 1,028 respectively.

24. Click **OK**.

The auto submit policy is created and listed in the View Auto Submit Policy page. When the events selected in the auto submit policy occur on the devices associated with the auto submit policy, incidents are automatically submitted to Juniper Support Systems (JSS) and a Technical support case is created. For Service Now operating in End Customer mode, the incidents are submitted to Service Now partner.

Service Now submit incidents for creating a case by using an auto submit policy only when the policy is enabled. By default, auto submit policies are enabled. To disable auto submit policies, see "Changing the Status of Auto Submit Policies" on page 247.

RELATED DOCUMENTATION

Assigning an Auto Submit Policy to a Device | 172

Changing the Dampening Status of an Auto Submit Policy | 250

Adding an SNMP Configuration to Service Now | 80

Creating and Editing a Notification Policy

Modifying an Auto Submit Policy

Junos Space Service Now provides the Modify option in the Actions list of the Auto Submit Policies page to modify auto submit policies. The Modify option lets you modify the following parameters of an auto submit policy:

- Devices assigned to the policy
- Dampening settings for the events included in the policy
- Auto submit filters associated with the policy
- Options such as priority, follow up method, dampening status, and delay time to submit the incidents

To modify an auto submit policy:

1. From the Service Now navigation tree, select **Administration** > **Auto Submit Policy**.
   The 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** list or the right-click menu.

   The Modify Auto Submit Policy page appears.

3. In the Choose devices to Include in Auto Submit Policy section select or clear the check boxes provided on the first column of the devices table to include or exclude the devices from the auto submit policy.

4. (Optional) Click the **Show Selected Devices** link to view devices selected for including in the auto submit policy.

5. Click **Next**.

   The Choose events to Include in Auto Submit Policy section appears.

6. (Optional) Modify the dampening settings of an incident by clicking the event on the dampening column and selecting a dampening value from the drop-down list.

   - *None*—Select None to create an incident for each occurrence of the events on the selected devices.
   - *Always*—Select Always if you do not want an incident to be created after the first occurrence of the event on the selected devices. Service Now does not create another incident for the event until the first incident is closed or deleted.
   - *Dampening intervals of 1 hr, 2 hr, 3 hr, and so on*—Service Now does not create incidents for the specified time duration after the first occurrence of the event. However, if the first incident is closed or deleted within in the specified time duration, Service Now creates another incident for the same event.

7. Click **Next**.

   The Choose filters to Include in Auto Submit Policy section appears.

8. (Optional) Select or clear the check boxes provided on the first column of the auto submit filters table to include or exclude the auto submit filters from the auto submit policy.

   If you want to associate a new filter with the auto submit policy, click the **Create Basic Filter** or **Create Advanced Filter** links to create a basic or advanced auto submit filter respectively.

9. (Optional) Click the **ReOrder Filters** link to reorder the filters.

10. Click **Save**.
    Your changes are saved and the auto submit policy is listed in the Auto Submit Policy page with your modifications.

RELATED DOCUMENTATION

Adding an SNMP Configuration to Service Now | **80**

Creating and Editing a Notification Policy

Assigning an Auto Submit Policy to a Device | **172**

Changing the Status of Auto Submit Policies

Service Now provides the Change Status option in the Actions list to enable or disable an auto submit policy. By default, an auto submit policy is enabled. Incidents can be submitted to Juniper Support Systems (JSS) or Service Now partner for creating a case only when an auto submit policy is enabled.

To change the status of auto submit policies:

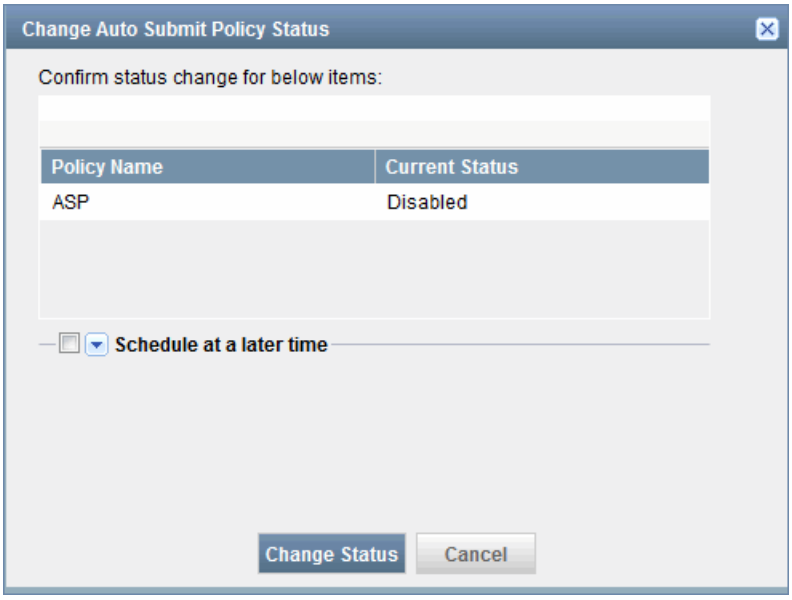
1. From the Service Now navigation tree, select **Administration** > **Auto Submit Policy**.

   The Auto Submit Policy page appears.

2. Select the auto submit policies for which you want to change the status and select **Change Status** from either the **Actions** list or the right-click menu.

   The **Change Auto Submit Policy Status** dialog box displays the current status of the selected auto submit policies. See Figure 47 on page 247.

Figure 47: Change Auto Submit Policy Status Page



3. (Optional) Click the **Schedule at a later time** check box and specify a date and time to enable the auto submit policy.

4. Click **Change Status**.
   If you have not scheduled a time for changing the status, Service Now initiates the job to change auto submit policy status immediately after you click Change Status and displays the jobs dialog box; otherwise, Service Now initiates the job at the scheduled time..

5. (Optional) Click the *Job ID*link to view the status of the change status job.

6. After the job is complete, click **OK**.

   The Quick View of the auto submit policy is displayed in the Auto Submit Policy page. .

RELATED DOCUMENTATION

- Modifying an Auto Submit Policy | **245**
- Changing the Dampening Status of an Auto Submit Policy | **250**
- Service Now Auto Submit Policy Overview | **237**
- Creating an Auto Submit Policy | **239**
- *Creating and Editing a Notification Policy*
- Adding an SNMP Configuration to Service Now | **80**

Deleting Auto Submit Policies from Service Now

Junos Space Service Now provides the Delete option in the Actions list of the Auto Submit Policies page to delete auto submit policies.

To delete auto submit policies:

1. From the Service Now navigation tree, select **Administration** > **Auto Submit Policy**.
   The Auto Submit Policy page appears.

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

   The Delete Policies dialog box appears.

3. Click **Delete** to confirm.

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

RELATED DOCUMENTATION

- Service Now Auto Submit Policy Overview | **237**

Creating an Auto Submit Policy | 239

Modifying an Auto Submit Policy | 245

Adding an SNMP Configuration to Service Now | 80

Creating and Editing a Notification Policy

Exporting an Incidents Report

Junos Space Service Now provides the Export Incident Report option in the Actions list of the Auto Submit Policies page to export details about incidents that Service Now submitted by using an auto submit policy.

Service Now exports the following information about an auto submit policy:

- Date and time the auto submit policy was used to submit an incident
- Event for which the auto submit policy was used to submit an incident
- Priority of the event
- Status of submitting the incident
- Host name, IP address, and the product family of the device on which the event occurred
- Version of AI-Scripts installed on the device

To export information about incidents associated with an auto submit policy:

1. From the Service Now navigation tree, select **Administration** > **Auto Submit Policy**.
   The Auto Submit Policy page appears.

2. Select one or more auto submit policies for which you want to export incident report to an Excel file, and click **Export Incidents Report** from either the **Actions** list or the right-click menu.

   The Export Incidents Report dialog box is displayed.

3. Click the **Click here to download Incidents for Auto Submit Policy above** link to generate the Excel file.

   The browser displays the dialog box for you to open or save the Excel file.

4. Select one of the following options:
   - To open the Excel file, select **Open with** and click **Open**.
   - 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, and click **OK**.

You can view the incidents created by selected auto submit policies in the generated Excel file.

RELATED DOCUMENTATION

Modifying an Auto Submit Policy | 245

Creating and Editing a Notification Policy

Adding an SNMP Configuration to Service Now | 80

Changing the Dampening Status of an Auto Submit Policy

Junos Space Service Now provides the Change Dampening option on the Actions list of the Auto Submit Policies page to change the dampening status for an auto submit policy. You can select one or multiple auto submit policies and change their dampening status (from Enabled to Disabled or vice versa).

Incidents are submitted for all events included in an auto submit policy only if the dampening status of the policy is enabled. However, you can configure Service Now to not submit an incident for an event included in the policy by setting the dampening status of the event to disabled. For information about modifying the dampening status of events in an event policy, see “Modifying an Auto Submit Policy” on page 245

To change the dampening status:

1. From the Service Now navigation tree, select **Administration** > **Auto Submit Policy**.

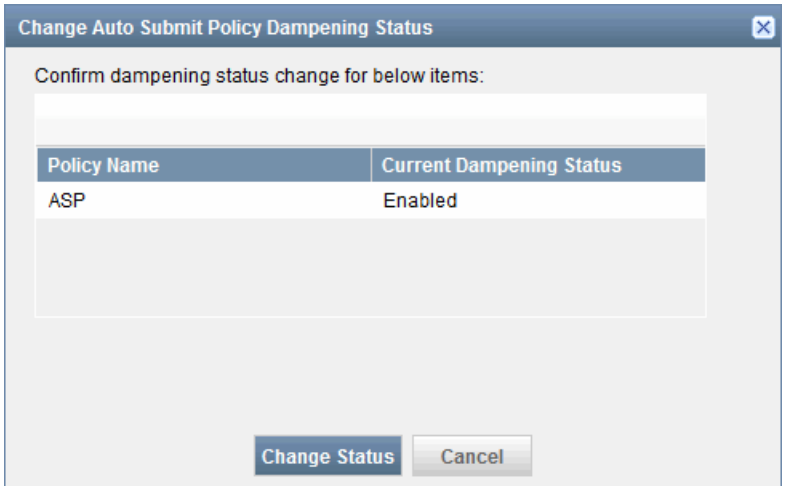
   The Auto Submit Policy page appears

2. Select one or more auto submit policies for which you want to change the dampening status.

3. Click **Change dampening status** from either the **Actions** list or the right-click menu.

   Service Now displays the Change Auto Submit Policy Dampening Status dialog box. See Figure 48 on page 251.

Figure 48: Change Auto Submit Policy Dampening Status Page



4. Click **Change Status**.

   The dampening status of the policy is changed.

RELATED DOCUMENTATION

Service Now Auto Submit Policy Overview | 237

Creating and Editing a Notification Policy

Adding an SNMP Configuration to Service Now | 80

12

CHAPTER

Managing Incident Filters

Service Now Incident Filters Overview | **255**

Viewing Incident Filters Configured on Junos Space Service Now | **257**

Creating Incident Filters | **258**

Modifying an Incident Filter | **264**

Exporting Incident Filters | **266**

Reordering Incident Filters | **267**

Enabling Incident Filters | **269**

Disabling Incident Filters | **270**

Deleting Incident Filters | **271**

Service Now Incident Filters Overview

Junos Space Service Now receives a Juniper Message Bundle (JMB) from a device, when an event occurs on the device, and creates an incident for the event. Starting in Service Now Release 17.1R1, incident filters provide you the option to select JMBs for which incidents can be created at a granular level. For information about incidents, see *Service Now Incidents Overview*.

You can use incident filters for the following purposes:

- Define the JMBs for which incidents should be created
- Define the JMBs for which incidents should not be created

Service Now displays all the configured incident filters on the Incident Filters page (**Administration > Incident Filters**).

When a JMB is received, Service Now applies the incident filter having the highest order, that is order 1, to it. If the JMB matches the term criteria of the filter, Service Now either creates an incident for the JMB or lists the JMB under Suppressed Events depending on the action defined in the filter. If the JMB does not match the term criteria of the filter with order 1, Service Now applies the incident filter with order 2. If the JMB matches the term criteria of the filter with order 2, Service Now creates an incident or lists the JMB under Suppressed Events depending on the action defined in the filter.

Service Now applies all the configured filters in the decreasing order till a match is found and performs the action specified in the matching filter. If no filter matches the JMB, Service Now performs the action defined in the Advanced Filter Settings under Global Settings.

Service Now provides options to define a basic filter or an advanced filter. You can also import filters to Service Now in XML format.

Basic filters filter JMBs based on attributes such as event synopsis, platform, event type and so on by using the *and* and *or* predefined computational logic. Advanced filters use Perl script to define the filtering logic and thereby provide the flexibility to define your own filtering logic.

Starting with Service Now Release 17.2R1, you can use in-built or custom Perl modules in advanced incident filters. For example, you can use custom Perl module for implementing a filtering logic and use that filtering logic across multiple advanced incident filters.

For using a Perl module, you can store the Perl module (***.pm**) in any desired location in the Junos Space server and ensure that the Perl module files have read and executable permissions and are accessible by the advanced filters.

Starting with Service Now 17.2R1 release, incident filters are stored at the **/var/cache/jboss/sn/advanced_filter** location of the Junos Space server.

NOTE: The Perl module in-built in Service Now includes an API, **getExistingIncidents()**, for getting information about the latest 20 incidents. The API is included in the **FilterUtilV1.pm file** stored in **/var/cache/jboss/SN/AdvancedFilters**. For more information, see "Sample Perl Script for Incident and Auto Submit Filters" on page 357.

NOTE:

- Incident filters cannot be applied to on-demand JMBs, BIOS JMBs, AIS Health Report JMBs, and Product Health Data JMBs
- In a Service Now partner, incident filters cannot be applied to JMBs received from a Service Now end customer.
- There is no limit on the number of filters that can be created. However, a large number of incident filters impacts the performance of Service Now when creating incidents.

Associated Actions

You can perform the following actions related to incident filters:

- View incident filters; see "Viewing Incident Filters Configured on Junos Space Service Now" on page 257 for details.
- Create incident filters; see "Creating Incident Filters" on page 258 for details.
- Modify incident filters; see "Modifying an Incident Filter" on page 264 for details.
- Export incident filters; see "Exporting Incident Filters" on page 266 for details.
- Reorder incident filters; see "Reordering Incident Filters" on page 267for details.
- Enable incident filters; see "Enabling Incident Filters" on page 269 for details.
- Disable incident filters; see "Disabling Incident Filters" on page 270details.
- Delete incident filters to a domain; see "Deleting Incident Filters" on page 271 for details.

Release History Table

Release	Description
17.1R1	Starting in Service Now Release 17.1R1, incident filters provide you the option to select JMBs for which incidents can be created at a granular level.

RELATED DOCUMENTATION

Service Now Auto Submit Filters Overview | 275

Service Now Incidents Overview

Submitting an Incident to Juniper Support Systems or Service Now Partner

Service Now Suppressed Events Overview

Viewing Incident Filters Configured on Junos Space Service Now

You can view incident filters that are configured on Junos Space Service Now on the Incident Filters page.

To view incident filters configured on Service Now, in the Service Now navigation tree, click **Administration > Incident Filters**. The Incident Filters page appears as shown in Figure 49 on page 257.

Figure 49: Incident Filters Page

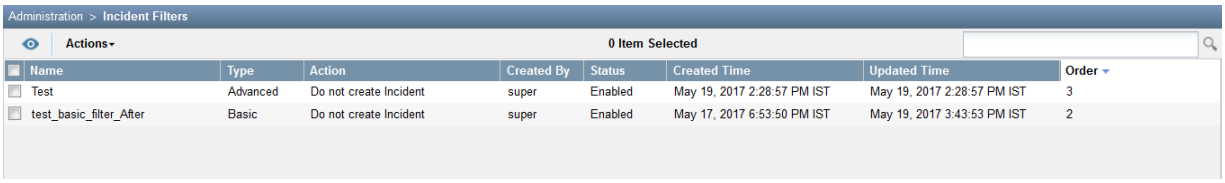


Table 23 on page 257 lists the information about Incident Filters displayed on the Incident Filters page.

Table 23: Fields in Incident Filters Page

Column	Description
Name	Name of the incident filter
Type	Type of filter: Basic or Advanced
Action	Action to be taken on a JMB when the JMB matches the conditions of the filter term: Create Incident or Do not create Incident
Created By	User who created the filter
Status	Status of the filter: Enabled or Disabled
Created Time	Date and time the filter was created

Table 23: Fields in Incident Filters Page *(continued)*

Column	Description
Updated Time	Date and time the filter was last updated
Order	Order in which the filters are applied to JMBs. By default, Service Now lists the filter with the highest order first. See "Reordering Incident Filters" on page 267 for details about changing the order of a filter.
Attributes	Link to view attributes defined in the filter

RELATED DOCUMENTATION

- Service Now Incident Filters Overview | 255
- Modifying an Incident Filter | 264
- Exporting Incident Filters | 266
- Reordering Incident Filters | 267
- Enabling Incident Filters | 269
- Disabling Incident Filters | 270
- Deleting Incident Filters | 271

Creating Incident Filters

IN THIS SECTION

- Creating a Basic Incident Filter | 259
- Creating an Advanced Incident Filter | 261
- Importing Incident Filters to Service Now | 263

This topic provides the details for creating basic and advanced filters and importing incident filters into Junos Space Service Now.

Creating a Basic Incident Filter

A basic incident filter uses the *and* and *or* predefined computational logic on the JMB attributes to filter a JMB. You can use the following JMB attributes to define a basic incident filter:

- Event Synopsis
- Description
- Device IP Address
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name

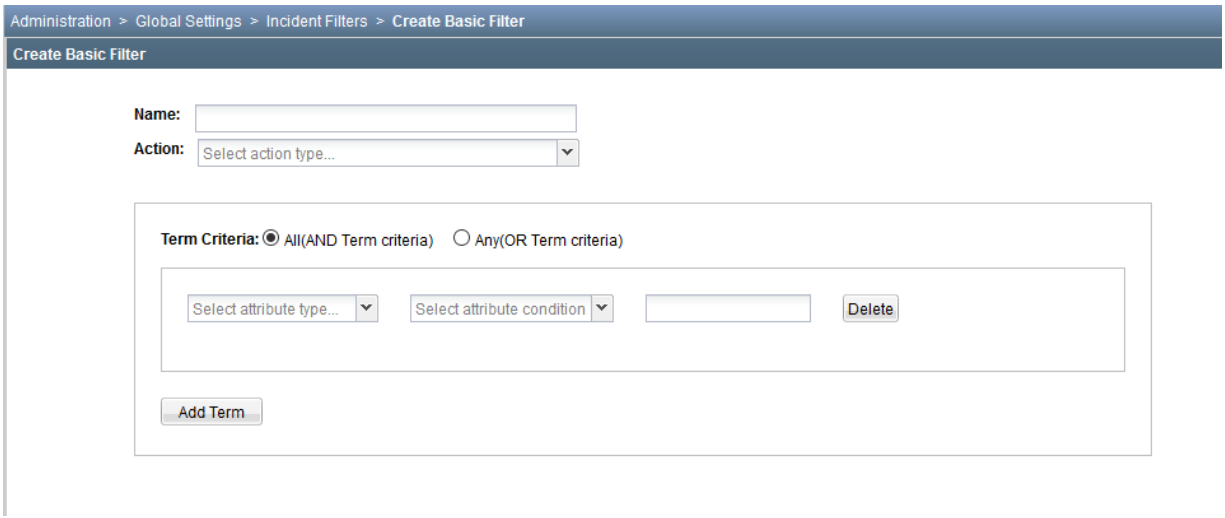
For example, you can have a basic incident filter to filter JMBs that have the event type set to *Daemon Crash* and the event synopsis does not contain the term *mgd*.

To create a basic incident filter:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Create Basic Filter**.

   The Create Basic Filter page appears as shown in Figure 50 on page 259.

Figure 50: Create Basic Filter Page for Creating Basic Incident Filters



2. In the **Name** text box, enter a name for the filter.

An incident filter name can have a maximum of 255 alphanumeric characters. Special characters are not allowed.

3. In the **Action** list, select an action for the filter:
   - Create Incident
   - Do Not Create an Incident
4. For **Term Criteria**, select one of the following:
   - All—An incident is created or not created for a JMB (depending on the selected action) only when the JMB matches all the terms defined in the filter.
   - Any—An incident is created or not created for a JMB (depending on the selected action) when the JMB matches any of the terms defined in the filter.
5. Select a JMB attribute from the list stating **Select attribute type**.
6. Select a condition from the list stating **Select attribute condition**.

   An attribute condition defines the conditions such as words that can be present or not present in an event synopsis, the date before or after which the event occurs, or specific platforms. The conditions listed in this drop-down list differ for each attribute.

   For example: The Platform attribute has conditions such as includes, does not include, and starts with.
7. Enter a value in the next text box for the attribute selected in step 5 and condition selected in step 6.

   For example, for the platform attribute, you can enter a value of SRX3400, EX3200, or MX960 so that the filter term is ”Platform includes SRX3400” or “Platform does not include SRX3400 ”.

   NOTE: You can add only one value for an attribute and a condition in the text box.
8. Click **Add Term** to add new filter terms and repeat steps 5 to 7.

   TIP: Click **Delete** to delete a filter term.
9. Click **Submit** to create the basic incident filter or click **Cancel** to cancel creating the filter.

   After you click Submit, Service now creates the filter and lists the newly created filter on the Incident Filters page.

Creating an Advanced Incident Filter

An advanced filter uses Perl scripts to define the filter terms and provides you the flexibility to define your own filtering logic. You can use the following JMB attributes to define a filter term in an advanced filter:

- Event Synopsis
- Description
- Junos OS Version
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name
- Device ID

"Perl script" on page 357 is an example of an advanced incident filter:

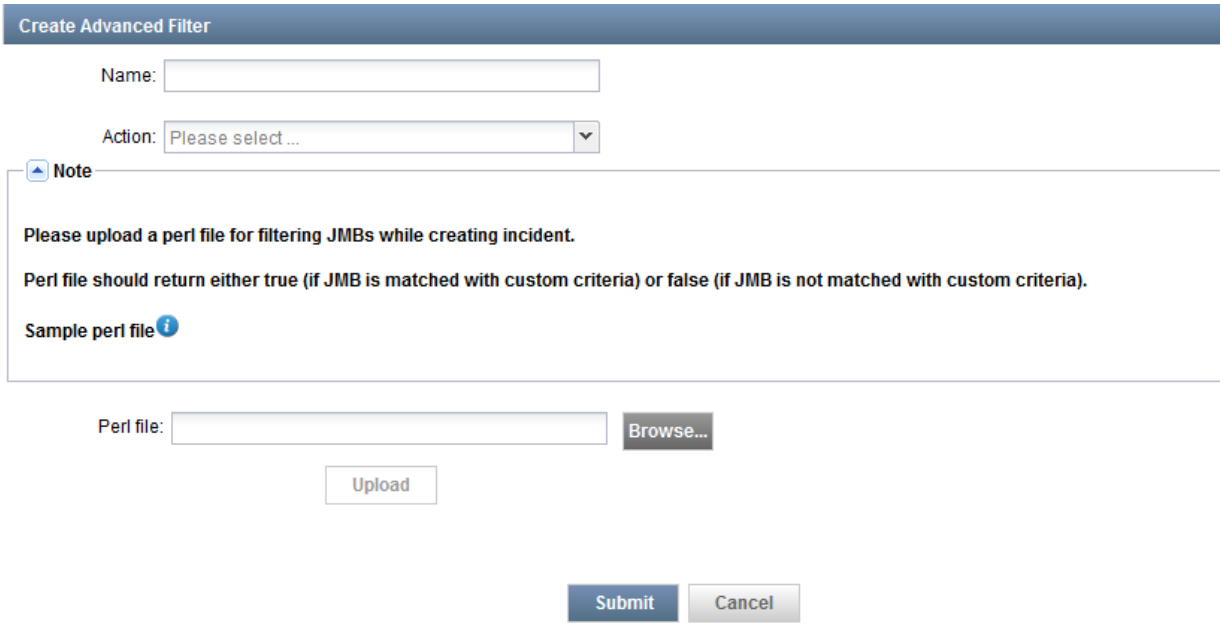
> **NOTE:** JMB attributes used in an advanced filter are assigned ARG values. For example , Device host name is assigned $ARGV[1]. Do not change the ARG value of a JMB attribute.

To create an advanced incident filter:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Create Advanced Filter**.

   The Create Advanced Filter page appears as shown in Figure 51 on page 262.

Figure 51: Create Advanced Filter Page for Creating Advanced Incident Filters



2. In the **Name** text box, enter a name for the filter.

   An incident filter name can have a maximum of 255 alphanumeric characters. Special characters are not allowed.

3. In the **Action** drop-down menu, select an action for the filter:

   - Create Incident
   - Do Not Create an Incident

4. (Optional) if the **Note** section is not expanded, click the down arrow icon next to Note to expand the Note section. The Note section provides a sample Perl script for filtering JMBs.

5. Click **Browse** and navigate to the Perl script on your local system.

   The Perl script should have the **.pl** extension.

6. Click **Upload** to upload the Perl script.

   When the upload is complete, Service Now displays a message indicating that the file is uploaded successfully.

Importing Incident Filters to Service Now

Service Now allows you to import both advanced and basic incident filters. You can use the import option to restore incident filters from an XML file in Service Now after an upgrade.

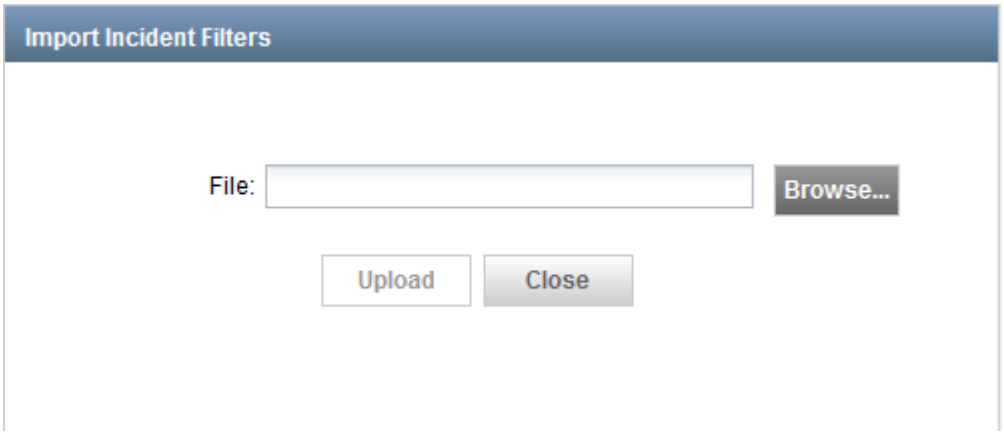
Imported filters are assigned the next available order, that is, when there are two filters in Service Now with orders 1 and 2, the imported filters are assigned order from 3 onwards.

To import incident filters to Service Now:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Import Incident Filters**.

   The Import Incident Filters dialog box appears as shown in Figure 52 on page 263.

Figure 52: Import Incident Filters Dialog Box



2. Click **Browse** and navigate to locate the file to be imported on your local system.

   The file to be imported should be in the ***.xml** format.

3. Select the file and click **Upload** to upload the incident filters.

   Service Now displays a message indicating that the file is uploaded successfully. You can view the uploaded filters on the Incident Filters page.

RELATED DOCUMENTATION

Service Now Incident Filters Overview | 255

Modifying an Incident Filter | 264

Exporting Incident Filters | 266

Reordering Incident Filters | 267
Enabling Incident Filters | 269
Deleting Incident Filters | 271
Service Now Auto Submit Filters Overview | 275

Modifying an Incident Filter

Junos Space Service Now provides Modify option on the Actions list on the Incident Filters page to modify an Incident filter. You can modify the following parameters of the incident filter:

- Name of the filter
- Filter action
- Filter terms

To modify an incident filter:

1. From the Service Now navigation tree, click **Administration > Incident Filters**.

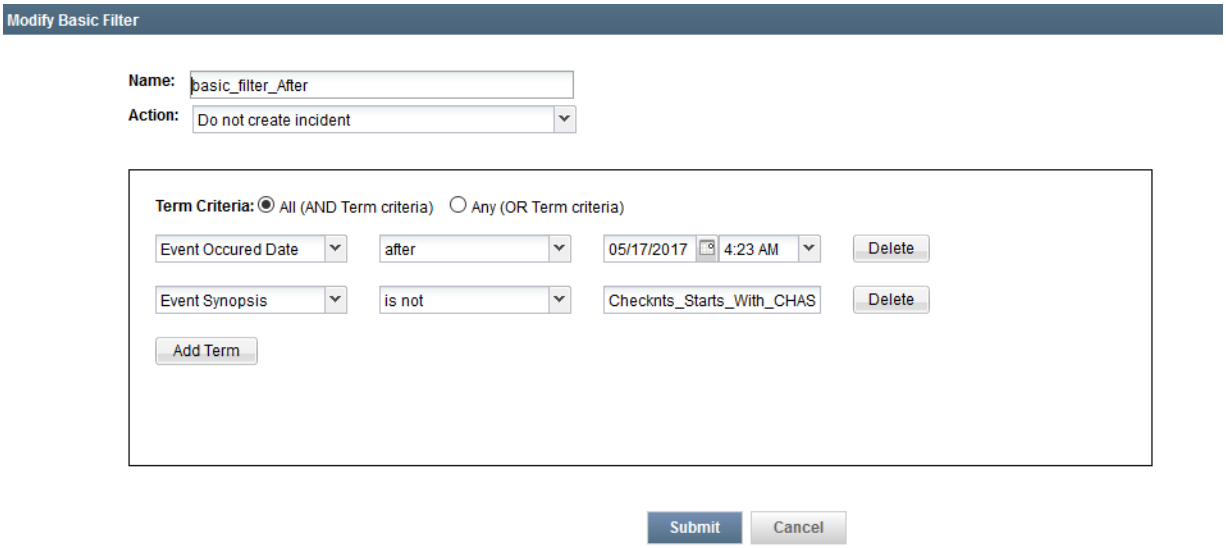
   The Incident Filters page appears.

2. Select the filter that you want to modify and select **Modify** from the Actions list or right-click menu.

   The Modify Basic Filter page or the Modify Advanced Filter page appears depending on the filter you chose to modify.

   Figure 53 on page 265 shows the Modify Basic Filter page for modifying basic incident filters.

Figure 53: Modify Basic Filter Page for Modifying a Basic Incident Filter



3. Modify the filter parameters—name, action, and filter terms.

   For an advanced filter, you can upload a new Perl script defining new terms to modfy one or more filter terms..

4. Click **Submit** to submit the changes.

   Service Now displays a message indicating successful modification of the incident filter.

RELATED DOCUMENTATION

- Service Now Incident Filters Overview | 255
- Viewing Incident Filters Configured on Junos Space Service Now | 257
- Creating Incident Filters | 258
- Exporting Incident Filters | 266
- Reordering Incident Filters | 267

Enabling Incident Filters | 269
Disabling Incident Filters | 270
Modifying an Auto Submit Filter | 283

Exporting Incident Filters

Service Now provides the Export option on the Actions list of the Incident Filters page to export all or selected incident filters. The filters are exported in the ***.xml** format.

To export one or more incident filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.

   The Incident Filters page appears.

2. Select one or more filters that you want to export and select **Export** from the Actions list or the right-click menu.

   The Export Incident Filters dialog box appears as shown in Figure 54 on page 266.

Figure 54: Export Incident Filters Dialog Box

3. Do one of the following to export one or more incident filters:
   - To export selected filters, click **Export Selected**.
   - To export all filters, click **Export All**.

   The Export Job Status dialog box appears. A **Download** link appears in the dialog box to download the XML file after the export job is complete.

4. Click the **Download** link to view or save the XML file on your local system.

The browser displays a dialog box to view or save the exported file.

5. Click the option to view the XML file or click the option to save the XML file on your local system.

RELATED DOCUMENTATION

Exporting Auto Submit Filters | 286
Service Now Incident Filters Overview | 255
Reordering Incident Filters | 267
Enabling Incident Filters | 269

Reordering Incident Filters

Order of a filter indicates the order in which a filter is applied to JMBs. A filter with order 1 is applied to a JMB before applying a filter with order 2. By default, a new filter is assigned the least order (highest number). Service Now provides the ReOrder Incident Filters option on the Actions list of the Incident filters page to re-order the incident filters.

To reorder incident filters:

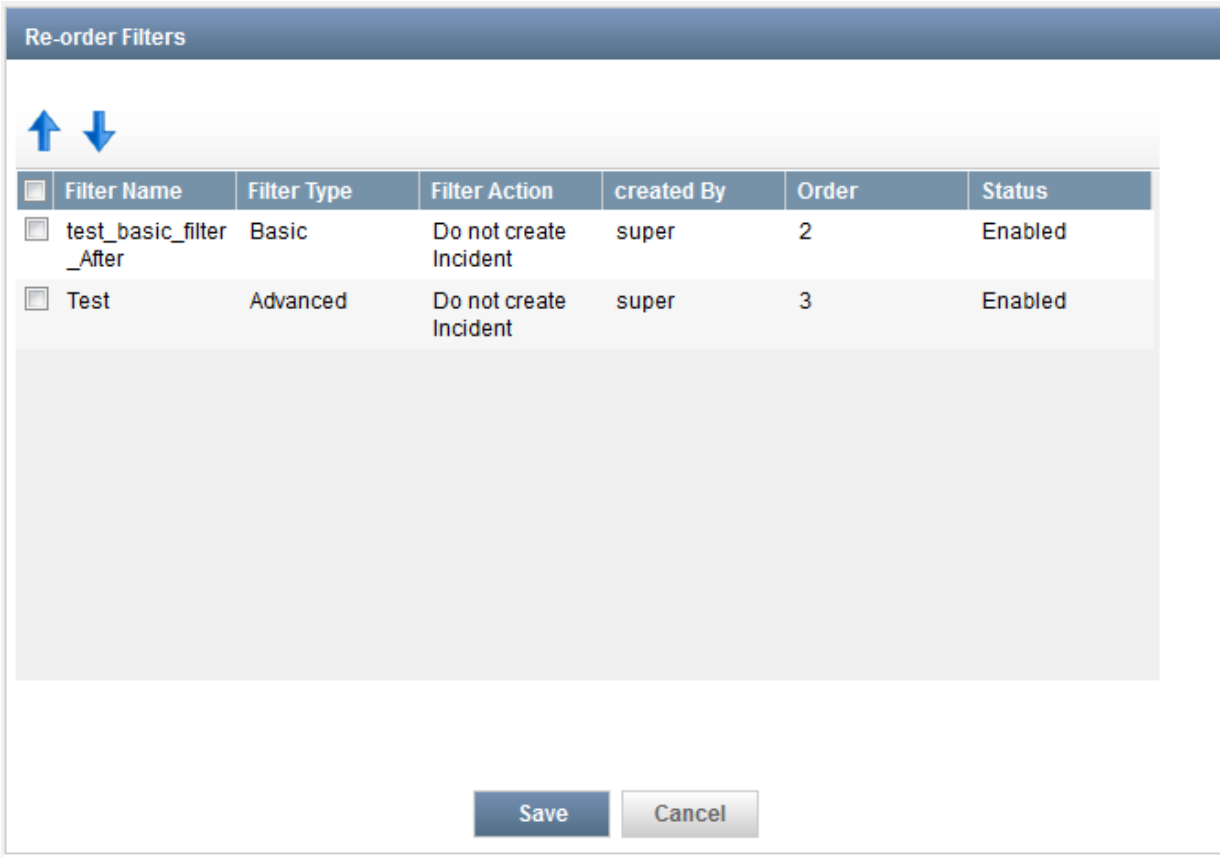
1. In the Service Now navigation tree, click **Administration > Incident Filters**.

   The Incident Filters page appears.

2. Select the filter and select **ReOrder Incident Filters** from the Actions list or right-click menu.

   The Re-order Filters page appears as shown in Figure 55 on page 268.

Figure 55: Re-order Filters page for Reordering Incident Filters



3. Select the filter that you want to reorder and select the up or down arrow present above the list of filters to move the filter in the upward or downward direction.

   As the filter is moved, its order also changes. The order of the filter increases when you move the filter in the upward direction and decreases when you move the filter in the downward direction.

4. Click **Save**.

   Service Now saves the new order of the filters and displays the new order on the Incident Filters page.

RELATED DOCUMENTATION

Service Now Incidents Overview

Service Now Incident Filters Overview | 255

Enabling Incident Filters

After you create an incident filter, you must enable the incident filter before it is applied to a JMB. Service Now provides the Enable option on the Actions list to enable incident filters. The Status column on the Incidents page displays whether the incident filter is enabled or disabled.

To enable one or more incident filters:

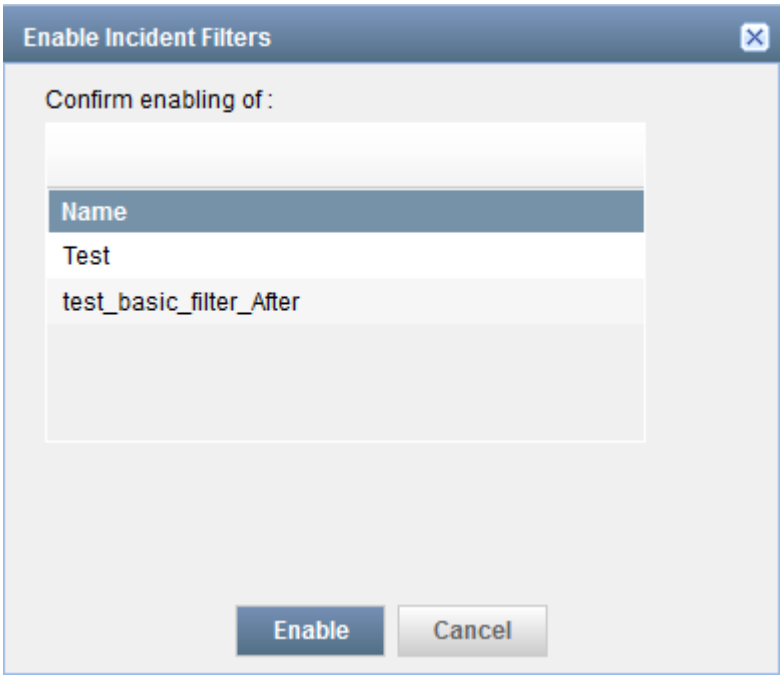
1. In the Service Now navigation tree, click **Administration > Incident Filters**.

   The Incident Filters page appears.

2. Select one or more filters that you want to enable and select **Enable** from the Actions list or right-click menu.

   The Enable Incident Filters dialog box appears as shown in Figure 56 on page 269.

Figure 56: Enable Incident Filters Dialog Box



3. Click **Enable** to enable the selected filters.

   Service Now changes the status of the selected filters to Enabled on the Incident Filters page.

RELATED DOCUMENTATION

Enabling Auto Submit Filters | 289
Disabling Incident Filters | 270
Deleting Incident Filters | 271
Service Now Incident Filters Overview | 255

Disabling Incident Filters

Service Now provides the Disable option on the Actions list to disable incident filters. A disabled filter cannot be used for filtering JMBs. Service Now displays whether an incident filter is enabled or disabled in the Status column of the Incident Filters page.

To disable one or more incident filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.

   The Incident Filters page appears.

2. Select one or more filters that you want to disable and select **Disable** from the Actions list or the right-click menu.

   The Disable Incidents Filters dialog box appears as shown in Figure 57 on page 270.

Figure 57: Disable incident Filters Dialog Box

3. Click **Disable** to disable the selected filters.

   Service Now changes the status of the filter to Disabled on the Incident Filters page.

RELATED DOCUMENTATION

- Disabling Auto Submit Filters | **291**
- Enabling Incident Filters | **269**
- Creating Incident Filters | **258**
- Service Now Incident Filters Overview | **255**

Deleting Incident Filters

Service Now provides the Delete option on the Action list to delete an Incident filter.

When you delete an incident filter, Service Now does not change the orders of the remaining filters.However, you can reorder the filters to change their order. For example, when there are four filters with orders 1, 2, 3, and 4 and if the filter with order 3 is removed, the remaining filters have the orders 1, 2, and 4.

To delete an incident filter:

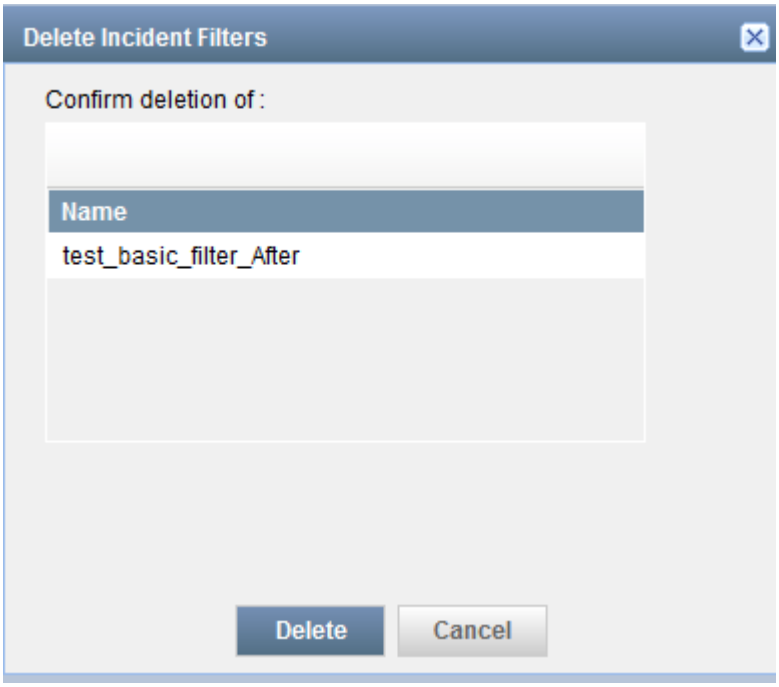
1. In the Service Now navigation tree, click **Administration > Incident Filters**.

   The Incident Filters page appears.

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

   The Delete Incident Filters dialog box appears as shown in Figure 58 on page 272.

Figure 58: Delete Incident Filters Dialog Box



3. Click **Delete** to delete the selected filters or click **Cancel** to cancel deleting the filters.

   Service Now displays a message indicating that the selected filters are deleted and the removes them from the Incident Filters page.

RELATED DOCUMENTATION

- Service Now Incident Filters Overview | 255
- Viewing Incident Filters Configured on Junos Space Service Now | 257
- Creating Incident Filters | 258
- Modifying an Incident Filter | 264
- Exporting Incident Filters | 266
- Reordering Incident Filters | 267
- Disabling Incident Filters | 270
- Deleting Auto Submit Filters | 292

13

CHAPTER

Managing Auto Submit Filters

Service Now Auto Submit Filters Overview | **275**

Creating Auto Submit Filters | **278**

Modifying an Auto Submit Filter | **283**

Exporting Auto Submit Filters | **286**

Reordering Auto Submit Filters | **287**

Enabling Auto Submit Filters | **289**

Disabling Auto Submit Filters | **291**

Deleting Auto Submit Filters | **292**

Service Now Auto Submit Filters Overview

Junos Space Service Now receives a Juniper Message Bundle (JMB) from a device, when an event occurs on the device, and creates an incident for the event. If auto submit policies are configured, Service Now automatically submits incidents to Juniper Support Systems (JSS) or Service Now partner for creating a case. Starting from Junos Space Service Now Release 17.1R1, you can assign auto submit filters to an auto submit policy to provide options for filtering incidents at a granular level before submitting them to JSS or a Service Now partner (in case of End Customer mode).

You can use the auto submit filters for the following purposes:

- Define incidents that should be submitted for creating cases
- Define incidents that should not be submitted for creating cases

Service Now displays all the configured auto submit policy filters on the Auto Submit Filters page (**Administration > Auto Submit Filters**) and provides options to define a basic filter, advanced filter, and import auto submit filters.

Basic filters filter incidents based on attributes such as event synopsis, platform, event type and so on by using the *and* and *or* predefined computational logic. Advanced filters use Perl script to define the filtering logic and thereby provide the flexibility to define your own filtering logic.

NOTE:

- Auto submit filters cannot be applied on incidents created for on-demand JMBs, BIOS JMBs, and Product Health Data JMBs.
- In a Service Now partner, auto submit filters cannot be applied to incidents received from a Service Now end customer.
- There is no limit on the number of auto submit filters that can be created. However, a large number of auto submit filters impacts the performance of Service Now when submitting incidents to JSS or Service Now partner.

Starting with Service Now Release 17.2R1, you can use in-built or custom Perl modules in advanced auto submit filters. For example, you can use custom Perl module for implementing a filtering logic and use that filtering logic across multiple advanced auto submit filters.

For using a Perl module, you can store the Perl module (***.pm**) in any desired location in the Junos Space server and ensure that the files have read and executable permissions and the files are accessible by the advanced filters.

Starting with Service Now 17.2R1 release, auto submit filters are stored at the **/var/cache/jboss/sn/advanced_filter**location of the Junos Space server.

NOTE: The Perl module in-built in Service Now includes an API, **getExistingIncidents()**, for getting information about the latest 20 incidents. The API is included in the **FilterUtilV1.pm file** stored in **/var/cache/jboss/SN/AdvancedFilters**. For more information, see "Sample Perl Script for Incident and Auto Submit Filters" on page 357.

To view auto submit filters configured on Service Now, in the Service Now navigation tree, click **Administration > Auto Submit Filters**. The Auto Submit Filters page appears as shown in Figure 59 on page 276. Double-clicking a filter opens the Auto Submit Filter Detail page that displays the details of the filter.

Figure 59: Auto Submit Filters Page

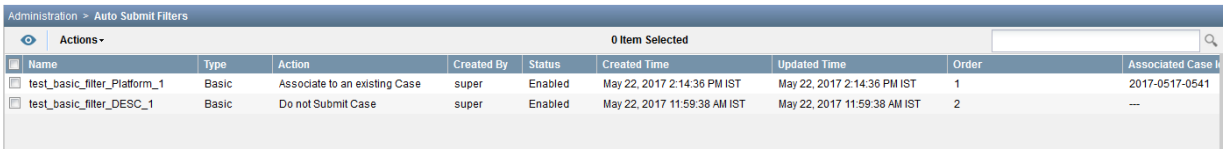


Table 24 on page 276 lists the attributes of the auto submit filter displayed on the Auto Submit Filters and Auto Submit Filter Detail page.

Table 24: Fields on Auto Submit Filters Page

Column	Description
Name	Name of the auto submit filter.
Type	Type of auto submit filter: Basic or Advanced.
Action	Action to be taken on an incident when the incident matches the conditions of the filter term: Submit case, Do not submit case, or Associate to an existing case.
Created By	User who created the filter.
Status	Status of the filter: Enabled or Disabled.
Created Time	Date and time when the filter is created.
Updated Time	Date and time when the filter was last updated.
Order	Order in which filters are applied to Incidents. By default, the filters are displayed in the ascending order. See "Reordering Auto Submit Filters" on page 287 for changing the order of a filter.

Table 24: Fields on Auto Submit Filters Page *(continued)*

Column	Description
Associated Case ID	ID of the case to which an incident should be associated.
Associated Policy	Auto submit policies in which the auto submit filter is used.
Attributes	Link to view attributes defined in the filter.

Actions That You Can Perform From the Auto Submit Filters Task

You can perform the following actions related to auto submit filters:

- View Auto Submit filters; see *Viewing Auto Submit Filters* for details.
- Create Auto Submit filters; see "Creating Auto Submit Filters" on page 278 for details.
- Modify Auto Submit filters; see "Modifying an Auto Submit Filter" on page 283 for details.
- Delete Auto Submit filters; see "Deleting Auto Submit Filters" on page 292 for details.
- Export Auto Submit filters; see "Exporting Auto Submit Filters" on page 286 for details.
- Reorder Auto Submit filters; see "Reordering Auto Submit Filters" on page 287 for details.
- Enable Auto Submit filters; see "Enabling Auto Submit Filters" on page 289 for details.
- Disable Auto Submit filters; see "Disabling Auto Submit Filters" on page 291 for details.

Release History Table

Release	Description
17.1R1	Starting from Junos Space Service Now Release 17.1R1, you can assign auto submit filters to an auto submit policy to provide options for filtering incidents at a granular level before submitting them to JSS or a Service Now partner (in case of End Customer mode).

RELATED DOCUMENTATION

Service Now Incident Filters Overview | 255

Service Now Suppressed Events Overview

Configuring Advanced Filter Settings | 92

Service Now Auto Submit Policy Overview | 237

Creating Auto Submit Filters

IN THIS SECTION

- Creating a Basic Auto Submit Filter | 278
- Creating an Advanced Auto Submit Filter | 280
- Importing Auto Submit Filters to Service Now | 282

This topic provides the details for creating basic and advanced filters and importing auto submit filters to Junos Space Service Now.

Creating a Basic Auto Submit Filter

A basic auto submit filter uses the the *and* and *or* predefined computational logic on the incident attributes to filter an incident for submitting to JSS or Service Now partner (in case of End Customer mode). You can use the following incident attributes to define a basic auto submit filter:

- Event Synopsis
- Description
- Device IP Address
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name
- Device ID

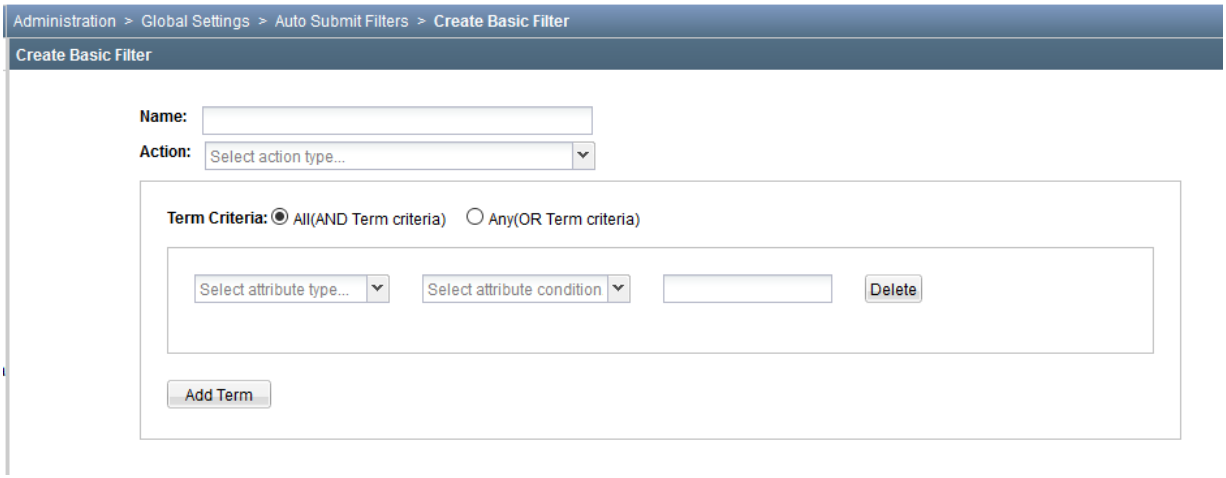
For example, you can have a basic auto submit filter to filter incidents that have event type set to *Daemon Crash* and the event synopsis does not contain the term *mgd*.

To create a basic auto submit filter:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters > Create Auto Submit Filter**.

   The Create Basic Filter page appears as shown in Figure 60 on page 279.

Figure 60: Create Basic Filter for Creating a Basic Auto Submit Filter



2. In the **Name** text box, enter a name for the filter.

   The name can have alphanumeric characters.

   The name of an auto submit filter can have a maximum of 255 alphanumeric characters. Special characters are not allowed.

3. In the **Action** list, select an action for the filter:
   - Submit Case
   - Do Not Submit Case
   - Associate to an Existing Case.
4. For **Term Criteria**, select a term criteria as follows:
   - All—The action defined in step 3 is performed only when the incident matches all the terms defined in the filter.
   - Any—The action defined in step 3 is performed only when the incident matches any of the terms defined in the filter.
5. Select an incident attribute from the list stating **Select an attribute type**.
6. Select a condition from the list stating **Select attribute condition**.

   An attribute condition defines the conditions such as words that can be present or not present for an attribute. The conditions listed in this list differ for each attribute.

For example, the Platform attribute has conditions such as includes, does not include, and starts with.

7. Enter a value in the next text box for the attribute selected in step 5 and condition selected in 6.

   For example, for the platform attribute, you can enter a value of SRX3400, EX3200, or MX960 so that the filter term is ”Platform includes SRX3400” or “Platform does not include EX3400”.

   > **NOTE:** You can add only one value for an attribute and a condition in the text box.

8. Click **Add Term** to add new filter terms and repeat steps 5 to 7.

   > **TIP:** Click **Delete** to delete a filter term.

9. Click **Submit** to create the basic auto submit filter.

   After you click submit, the filter is created and listed on the Auto Submit Filters page.

Creating an Advanced Auto Submit Filter

An advanced filter uses Perl scripts to define the filter terms and provides you the flexibility to define your own filtering logic. You can use the following incident attributes to define a filter term in an advanced filter:

- Event Synopsis
- Description
- Junos OS Version
- Event Occurred Date
- Platform
- Event Type
- Entity
- Device Name

“Perl script” on page 357 is a an example of an advanced auto submit filter:

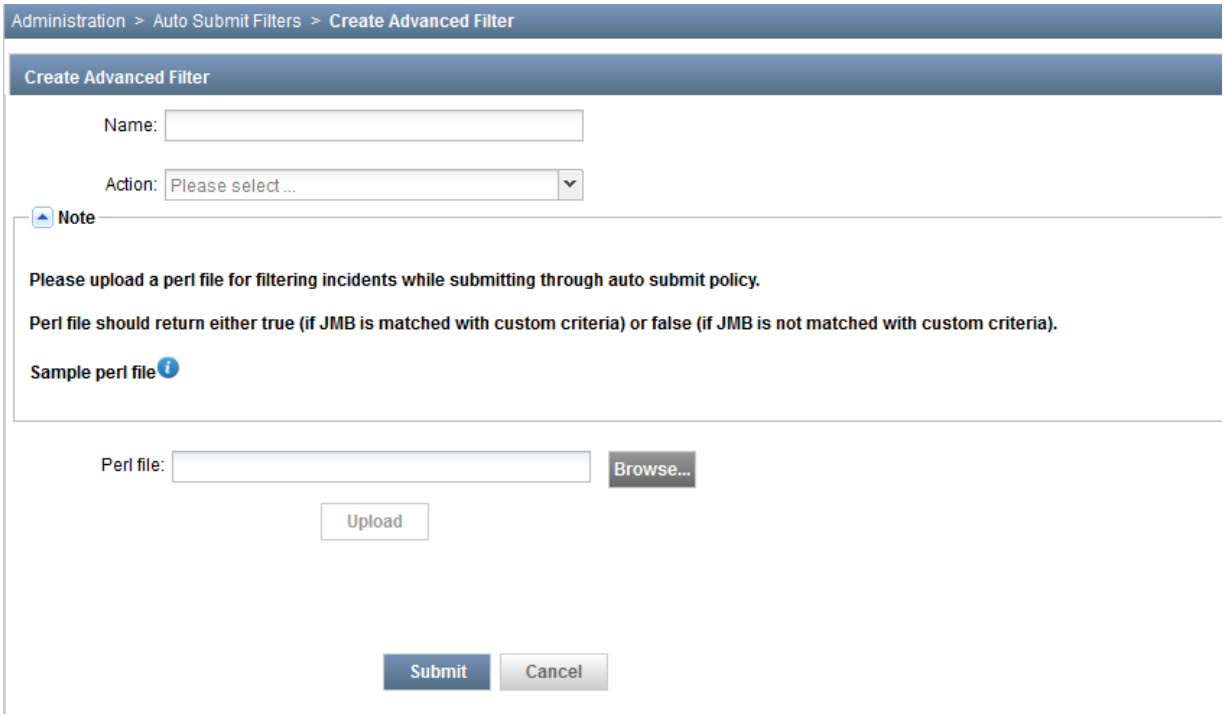
NOTE: JMB attributes used in an advanced filter are assigned ARG values. For example , Device host name is assigned $ARGV[1]. Do not change the ARG value of a JMB attribute.

To create an advanced auto submit filter:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Create Advanced Filter**.

   The Create Advanced Filter page appears as shown in Figure 61 on page 281.

Figure 61: Create Advanced Filter Page for Creating an Advanced Filter



2. In the **Name** text box, enter a name for the filter.

   The name of an auto submit filter can have a maximum of 255 alphanumeric characters. Special characters are not allowed.

3. In the **Action** list, select an action for the filter:

   - Submit Case
   - Do Not Submit Case
   - Associate to an Existing Case.

4. (Optional) If the **Note** section is not expanded, click the down arrow icon next to Note to expand the Note section.

   The Note section provides a sample Perl script for filtering JMBs.

5. Click **Browse** and navigate to the Perl script stored on your local system.

   The Perl script should have the extension **.pl**.

6. Click **Upload** to upload the Perl script.

   When the upload is complete, a message indicating that the file is uploaded successfully is displayed.

Importing Auto Submit Filters to Service Now

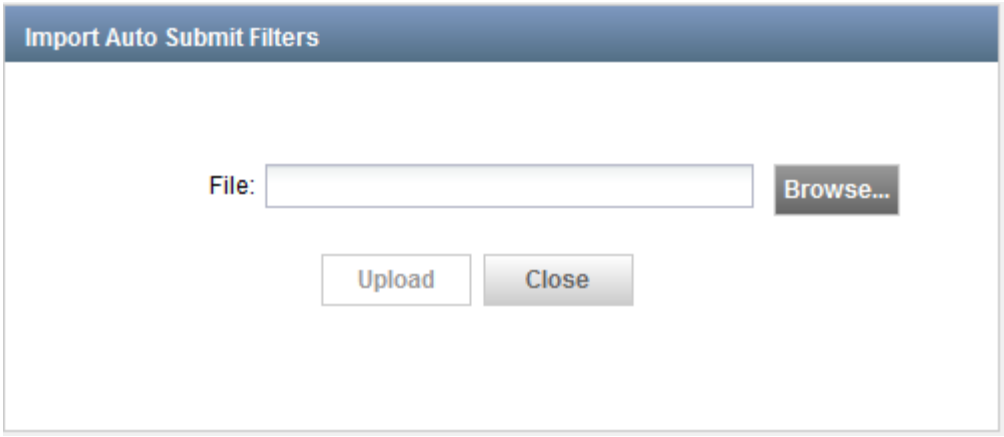
Service Now allows you to import both advanced and basic auto submit filters. You can use the import option to restore filters from an XML file in Service Now after an upgrade.

To import auto submit filters to Service Now:

1. In the Service Now navigation tree, click **Administration > Incident Filters > Import Incident Filters**.

   The Import Auto Submit Filters dialog box appears as shown in Figure 62 on page 282.

Figure 62: Import Auto Submit Dialog Box



2. Click **Browse** and navigate to locate the file to be imported on your local system.

   The file to be imported should be in the ***.xml** format.

3. Select the file and click **Upload** to upload filters.

A message indicating that the file is uploaded successfully is displayed.

RELATED DOCUMENTATION

Creating Incident Filters | 258

Service Now Auto Submit Filters Overview | 275

Modifying an Auto Submit Filter

Junos Space Service Now provides the Modify option on the Actions list of the Auto Submit Filters page to modify an auto submit filter. You can modify the following parameters of the auto submit filter:

- Name of the filter
- Filter action
- Filter terms

To modify an auto submit filter:

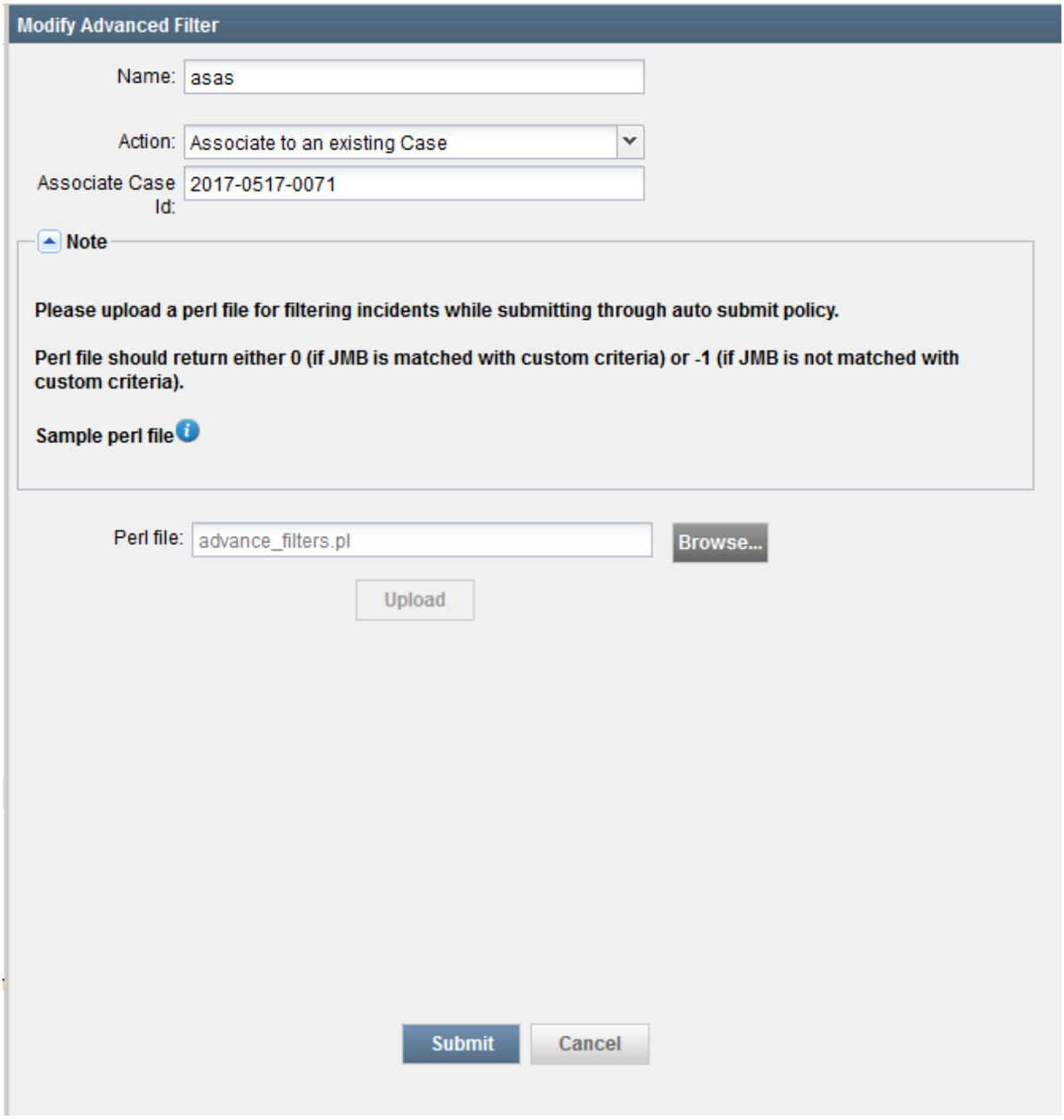
1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

   The Auto Submit Filters page appears.

2. Select the filter that you want to modify and select **Modify** from the Actions list or right-click menu.

   The Modify Basic Filter or Modify Advanced Filter page appears depending on the filter you chose to modify. The Modify Advanced Filter page is shown in Figure 63 on page 284.

Figure 63: Modify Advanced Filter Page for Modifying an Advanced Auto Submit Filter



3. Modify the filter parameters:
   - Name
   - aAction
   - Associate Case Id if Action is set to Associate to an Existing Case
   - Filter Terms

For an advanced filter, you can upload a new Perl script defining new terms to modify the filter term parameters.

4. Click **Submit** to submit the changes or click **Cancel** to cancel the changes.

   A message indicating that the auto submit filter is successfully modified is displayed.

RELATED DOCUMENTATION

- Modifying an Incident Filter | **264**
- Exporting Auto Submit Filters | **286**
- Reordering Auto Submit Filters | **287**
- Deleting Auto Submit Filters | **292**

Exporting Auto Submit Filters

Junos Space Service Now provides the Export option on the Actions list of the Auto Submit Filters page to export all the configured or selected auto submit filters. The filters are exported in the ***.xml** format.

```
<Filters>
    <snVersion>18.1R1</snVersion>
    <Filter>
        <FilterData>
            <created>1514896801840</created>
            <createdBy>super</createdBy>
            <domainId>2</domainId>
            <filterAction>2</filterAction>
            <filterName>Test</filterName>
            <filterSubAction>4</filterSubAction>
            <filterType>1</filterType>
            <lastUpdated>1514896801840</lastUpdated>
            <priority>1</priority>
            <status>1</status>
        </FilterData>
        <FilterAttributes>
            <FilterAttribute>
                <domainId>2</domainId>
                <filterAttributeCondition>starts with</filterAttributeCondition>
                <filterAttributeName>Entity</filterAttributeName>
                <filterAttributeValue>r</filterAttributeValue>
                <filterCondition>1</filterCondition>
                <filterId>53475</filterId>
                <priority>0</priority>
            </FilterAttribute>
        </FilterAttributes>
        <FilterFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:nil="true"/>
    </Filter>
</Filters>
```

To export one or more auto submit filters:

1. In the Service Now navigation tree, click **Administration > Incident Filters**.

   The Auto Submit Filters page appears.

2. Select one or more filters that you want to export and select **Export** from the Actions or the right-click

menu.

The Export Auto Submit Filters dialog box appears as shown in Figure 64 on page 287.

Figure 64: Export Auto Submit Filters Dialog Box

3. Do one of the following:
   - To export the selected filters, click **Export Selected**.
   - To export all filters, click **Export All**.

   The Export Job Status dialog box appears. A **Download** link appears on the dialog box to download the XML file after the export job is complete.

4. Click the **Download** link to view or save the XML file on your local system.

   The browser displays the dialog box to view or save the exported file.

5. View or save the XML file on your local system.

Reordering Auto Submit Filters

Order of a filter indicates the order in which a filter is applied to incidnets. A filter with order 1 is applied to an incident before applying a filter with order 2. By default, a new filter is assigned the least order (highest order number). Service Now provides the ReOrder Auto Submit Filters option on the Actions list of the Auto Submit Filters page to reorder the auto submit filters.

To reorder an auto submit filter:

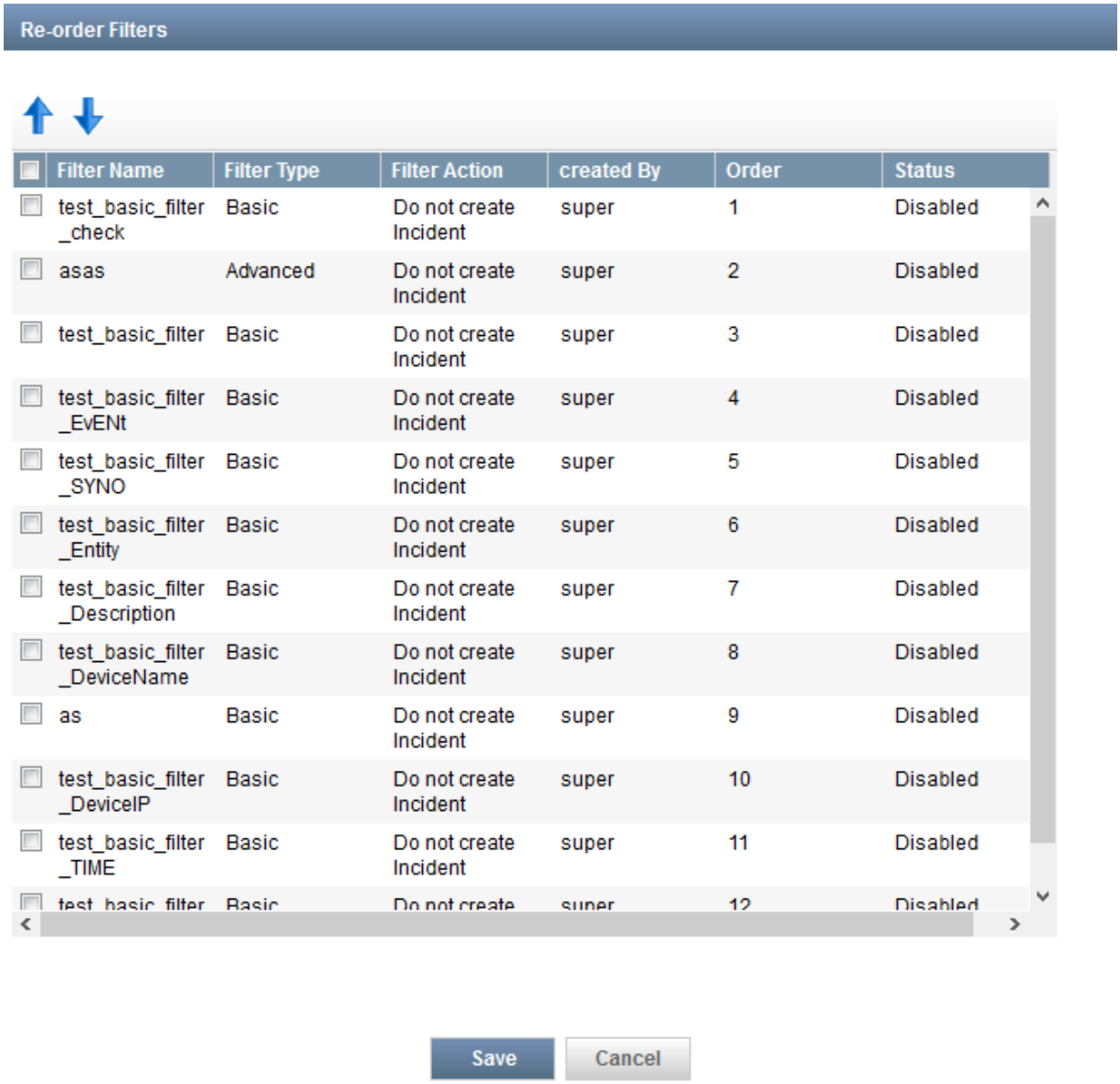
1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

   The Auto Submit Filters page appears.

2. Click **Actions > ReOrder Auto Submit Filters**.

   The Re-order Filters dialog box appears as shown in Figure 65 on page 288.

Figure 65: Re-order Filters Dialog Box for Reordering Auto Submit Filters



3. Select the filter that you want to reorder and select the up or down arrow present above the list of filters to move the filter in the upward or downward direction.

   As the filter is moved, its order also changes. The order of the filter increases when the filter is moved in the upward direction and decreases when the filter is moved in the downward direction.

4. Click **Save**.

   The new order of the filters is saved and displayed on the Auto Submit Filters page.

RELATED DOCUMENTATION

Reordering Incident Filters | 267

Modifying an Auto Submit Policy | 245

Service Now Auto Submit Filters Overview | 275

Enabling Auto Submit Filters

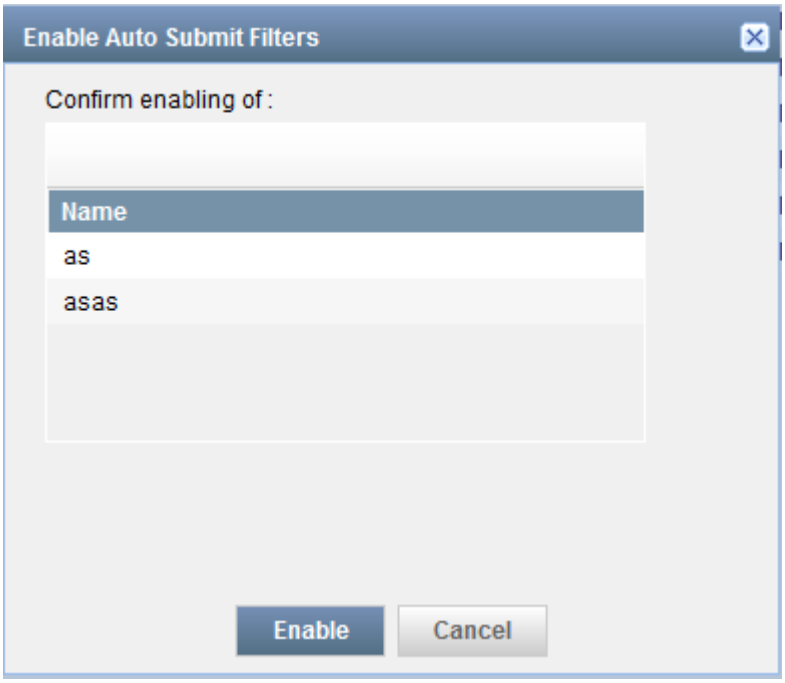
After you create an auto submit filter, you must enable the filter before it is applied to an incident. Service Now provides the Enable Auto Submit Filters option on the Actions list of the Auto Submit Filters page to enable auto submit filters. The Status column on the Auto Submit Filters page displays whether the auto submit filter is enabled or disabled.

To enable one or more auto submit filters:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

   The Auto Submit Filters dialog box appears as shown in Figure 66 on page 290.

Figure 66: Enable Auto Submit Filters Dialog Box



2. Select one or more filters that you want to enable and select **Enable Auto Submit Filters** from the Actions or the right-click menu.

   The Enable Auto Submit Filters dialog box appears.

3. Click **Enable** to enable the selected filters.

   The status of the selected filter changes to Enabled on the Auto Submit Filters page.

RELATED DOCUMENTATION

- Enabling Incident Filters | 269
- Reordering Auto Submit Filters | 287
- Disabling Auto Submit Filters | 291
- Service Now Auto Submit Policy Overview | 237
- Service Now Auto Submit Filters Overview | 275

Disabling Auto Submit Filters

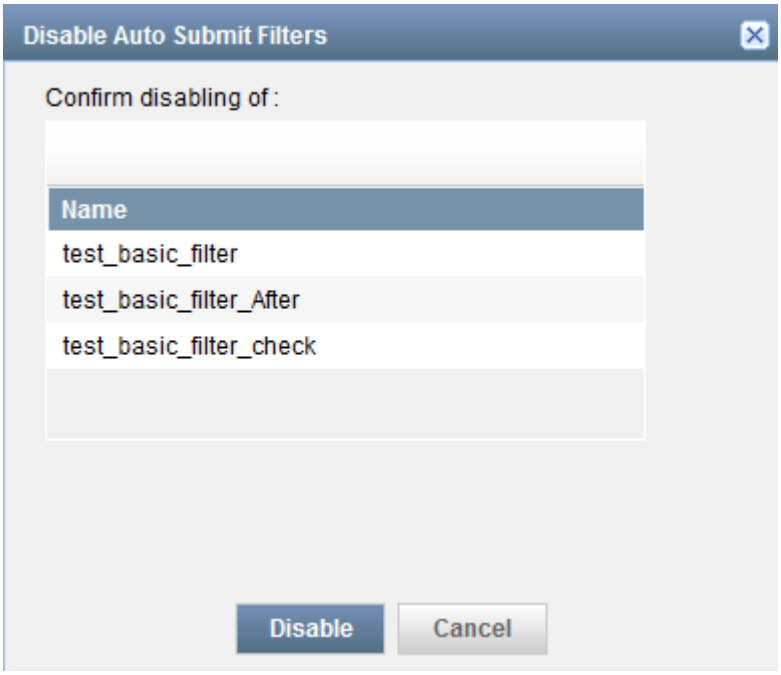
Junos Space Service Now provides the Disable Auto Submit Filters option on the Actions list of the Auto Submit Filters page to disable auto submit filters. A disabled filter cannot be used for filtering incidents for submitting to Juniper Support Systems (JSS) or Service Now partner.

To disable one or more auto submit filters:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

   The Auto Submit Filters dialog box appears as shown in Figure 67 on page 291.

Figure 67: Disable Auto Submit Filters Dialog Box



2. Select one or more filters that you want to enable and select **Disable** from the Actions list or the right-click menu.

   The Disable Auto Submit Filters dialog box appears.

3. Click **Disable** to disable the selected filters.

   The status of the selected filters is changed to disabled on the Auto Submit Filters page.

RELATED DOCUMENTATION

Deleting Auto Submit Filters

Junos Space Service Now provides the Delete option on the Actions list of the Auto Submit Filters page to delete auto submit filters from the Auto Submit Filters page.

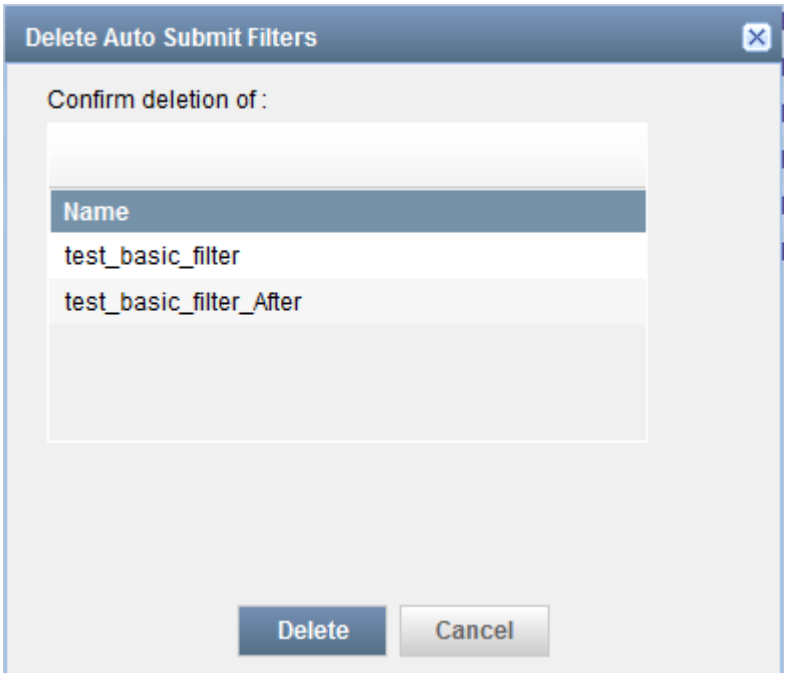
> **NOTE:** You cannot delete an auto submit filter if it is associated with an auto submit policy. Therefore, before you attempt deleting an auto submit policy, ensure that filter that you are going to delete is not associated with any auto submit policy.

To delete an auto submit filter:

1. In the Service Now navigation tree, click **Administration > Auto Submit Filters**.

   The Auto Submit Filters dialog box appears as shown in Figure 68 on page 292.

Figure 68: Delete Auto Submit Filters Dialog Box



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

The Delete Auto Submit Filters dialog box appears.

3. Click **Delete** to delete the selected filters or click **Cancel** to cancel deleting the filters.

   Service Now displays a message indicating that the auto submit filters are deleted successfully and removes the deleted filters from the Auto Submit Filters page.

RELATED DOCUMENTATION

Service Now Auto Submit Filters Overview | 275

14

CHAPTER

Configuring and Managing Product Health Data Collection

Product Health Data Collection Configuration Overview | **297**

Configuring Product Health Data Collection on a Device | **300**

Viewing Product Health Data Files Collected from a Device | **307**

Modifying a Product Health Data Collection Configuration | **310**

Rescheduling a Product Health Data Collection Configuration | **313**

Retrying Collecting Product Health Data from a Device | **315**

Disabling Product Health Data Collection on a Device | **316**

Enabling Product Health Data Collection on a Device | **317**

Aborting a Product Health Data Collection Configuration | **319**

Exporting Product Health Data Information to an Excel File | **321**

Deleting Product Health Data Files Collected from a Device | **327**

Deleting a Product Health Data Collection Configuration from Service Now | **329**

Product Health Data Collection Configuration Overview

Starting from Service Now Release 15.1R1, Service Now provides the Product Health Data Collection feature to collect product health data (PHD) from managed devices for assessing devices' health. PHD is collected from a device by executing predefined Junos OS commands. For information about the Junos OS commands used for collecting PHD, see Commands Used for Collecting PHD from Managed Devices

You can configure Product Health Data Collection (PHDC) on Service Now operating in Direct, or Partner Proxy modes. Starting in Service Now Release 16.1R1, Service Now can collect PHD when operating in End Customer mode as well. However, uploading the end-customer product health data to Service Now partner is not supported.

NOTE: A Service Now partner cannot configure PHDC on end-customer devices.

Product health data collection (PHDC) is configured on Service Now by defining the following parameters:

- Devices on which PHD should be collected
- Number of days for which PHD should be collected
- Whether PHD data should be submitted to Juniper Support Systems (JSS) or Service Now partner
- Whether PHD data should be deleted from Service Now once uploaded to JSS or Service Now partner
- Whether IP addresses should be overwritten with asterisks (*) in the PHD files

PHDC configurations on Service Now can be viewed on the Product Health Data Collection page (**Administration > Product Health Data Collection**) as shown in Figure 69 on page 297.

Figure 69: Product Health Data Collection Page

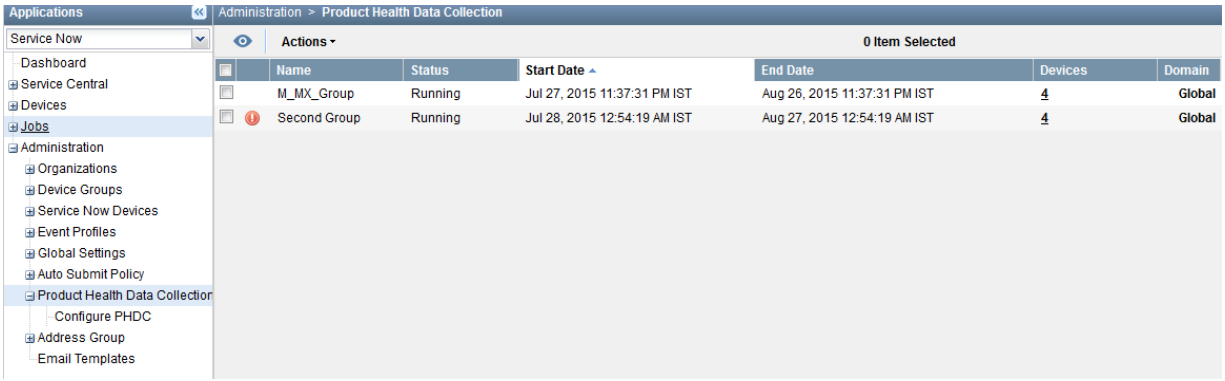


Table 25 on page 298 lists the fields on the Product Health Data Collection page.

Table 25: Fields on the Product Health Data Collection Page

Field Name	Description
Name	Name of the PHDC configuration
Status	Status of the PHDC configuration Possible values are: • Scheduled—PHD is scheduled to be collected from all devices assigned to the PHDC configuration at the scheduled time. • Starting—PHD collection is starting on all devices included in the PHDC configuration. • Running—PHD is being collected from all devices included in the configuration. • Failed—PHD collection failed in one or more devices included in the configuration. • Stopping—PHD collection is being stopped on one or more devices included in the configuration. • Stopped—PHD collection is stopped on one or more devices in included in the configuration. • Enabling—PHD collection is being enabled on one or more devices in the configuration after being disabled. • Disabling—PHD collection is being disabled on one or more devices in the configuration. • Aborting—PHD collection is being aborted on all devices of the configuration.
Start Date	Date and time PHD collection is scheduled to start or the date and time when PHD collection started
End Date	Date and time to end PHD collection or PHD collection ended (if the PHDC status is completed)
Devices	Number of devices included in the PHDC configuration Click the link to view the details of devices, the status of PHD collection on the devices and view the PHD files collected from individual devices. See *Service Now Product Health Data Collection Overview* for details on the status of PHD collection on a device.
Domain	Domain to which the PHDC configuration is assigned By default, a PHDC configuration is assigned to the domain in which the user creating the PHDC configuration is logged in.

Benefits of Product Health Data Collection

The Product Health Data Collection (PHDC) feature helps to confirm whether managed devices are maintaining performance expectations based on best practices recommended by Juniper Networks. The PHDC feature identifies potential malfunctioning of hardware components, dormant problems, any abnormalities in the trend data for improvement and any other performance related issues. Engineers at Juniper Networks analyze the product health data and recommend actions to customers to identify potential risks and issues with their devices before impacting their network and proactively improve network performance.

Actions That You Can Perform From the Product Health Data Collection Task

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

- Modify a PHDC configuration; see "Modifying a Product Health Data Collection Configuration" on page 310 for details.
- Reschedule a PHDC configuration; see "Rescheduling a Product Health Data Collection Configuration" on page 313 for details.
- Retry collecting PHD from devices on which an earlier attempt to collect PHD failed; see "Retrying Collecting Product Health Data from a Device" on page 315 for details.
- Enable PHD collection on devices; see "Enabling Product Health Data Collection on a Device" on page 317 for details.
- Disable PHD collection on devices; see "Disabling Product Health Data Collection on a Device" on page 316 for details.
- Abort PHD collection on devices; see "Aborting a Product Health Data Collection Configuration" on page 319 for details.
- Delete a PHDC configuration; see "Deleting a Product Health Data Collection Configuration from Service Now" on page 329 for details.
- Assign a PHDC configuration to another domain; see "Assigning a Service Now Object to Another Domain" on page 56 for details.

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16.1R1, Service Now can collect PHD when operating in End Customer mode as well
15.1R1	Starting from Service Now Release 15.1R1, Service Now provides the Product Health Data Collection feature to collect product health data (PHD) from managed devices for assessing devices' health.

RELATED DOCUMENTATION

Configuring Product Health Data Collection on a Device | 300

Service Now Product Health Data Collection Overview

Configuring Product Health Data Collection on a Device

IN THIS SECTION

- Configuring PHDC by Using the Product Health Data Collection Task | 300
- Configuring PHDC by Using the Service Now Devices Task | 303

Product health data collection (PHDC) configurations are listed on the Product Health Data Collection page of the Administration workspace.

Junos Space Service Now provides the following methods to configure PHDC on managed devices:

Configuring PHDC by Using the Product Health Data Collection Task

Configuring PHDC from Product Health Data Collection task involves selecting devices on which to configure PHDC and then configuring the parameters.

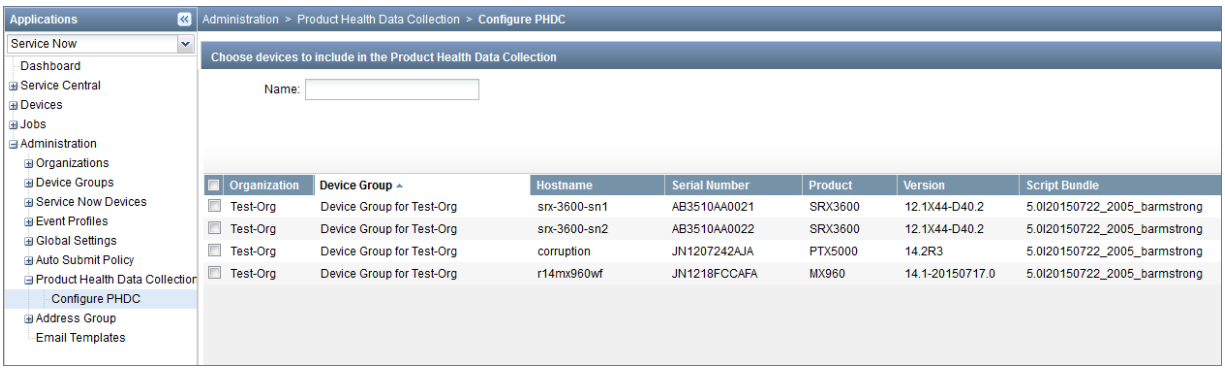
NOTE: PHDC consumes CPU cycles and disk resources of the device. Therefore, performance of the device might be affected while PHD is being collected.

To configure PHDC on a device from the Product Health Data Collection task:

1. From the Service Now navigation tree, select **Administration > Product Health Data Collection > Configure PHDC**.

   The Configure PHDC page appears as shown in Figure 70 on page 301.

Figure 70: Configure PHDC Page



2. Enter a name for the PHDC configuration.

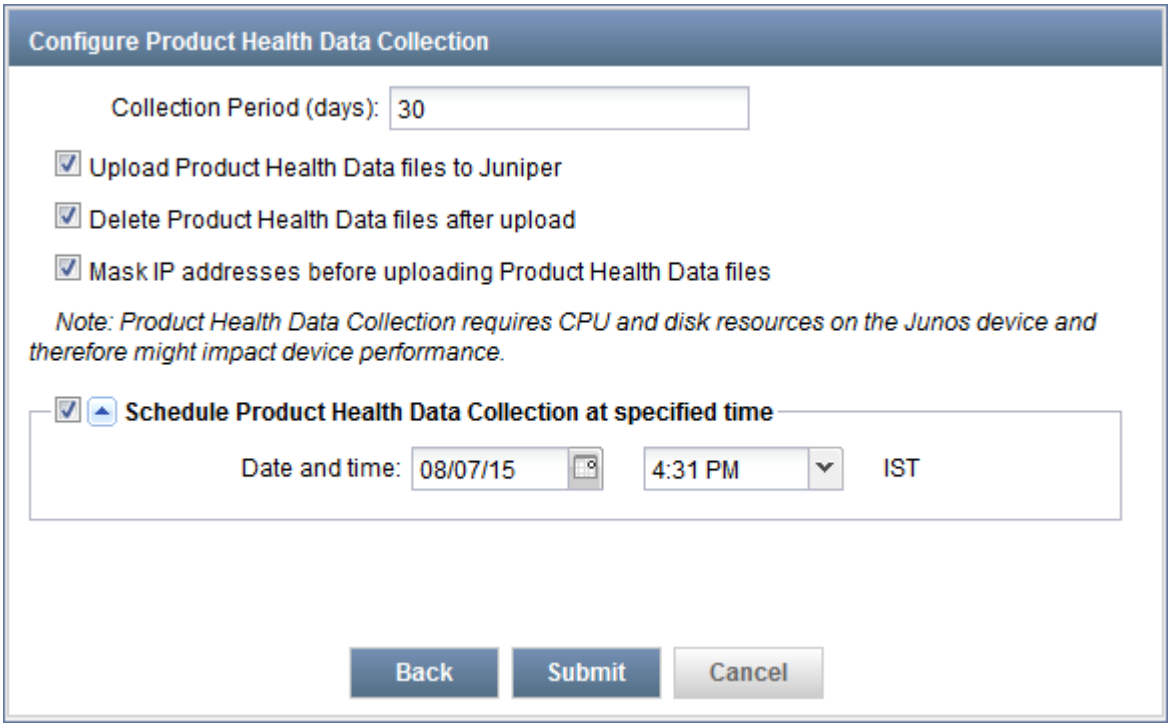
   The name of a PHDC configuration must have 4 to 64 alphanumeric characters. You can use underscore (_) and hyphen (-) as special characters.

3. Click on the devices that you want to include in the PHDC configuration. Alternatively, select the check box next to the **Organization** field to include all devices listed in the PHDC configuration.

4. Click **Next**.

   The Configure Product Health Data Collection page appears as shown in Figure 71 on page 302.

Figure 71: Configure Product Health Data Collection



5. On the Configure Product Health Data Collection page, configure options as follows:

   - **Collection Period (days)**: Enter the number of days when product health data (PHD) should be collected from the devices.

     Number of days can range from 1 to 90. The default value is 30 days.

   - **Upload Product Health Data files to Juniper**: Select this check box to upload PHD files collected from devices to Juniper Support Systems (JSS).

     This option is selected by default.

     > **NOTE:** If you clear this check box, PHD files are not uploaded to JSS. If required later, you cannot upload PHD files to JSS.

   - **Delete Product Health Data files after upload**: Select this check box to delete PHD files from a device immediately after they are uploaded to JSS.

     This option is selected by default.

> **NOTE:** If you clear this check box, PHD files are automatically deleted four days after the files are collected by Service Now.

- **Mask IP addresses before uploading Product Health Data files**: Select this check box to replace IP addresses with asterisks (*) in collected PHD.

  This option is selected by default.

- (Optional) **Schedule PHD Collection at specified time**: Select this check box to schedule a date and time for collecting PHD from the selected devices.

6. Click **Submit** to submit the PHDC configuration.

   The PHDC configuration is listed on the Product Health Data Collection page.

   If a date and time is not scheduled for PHD collection, Service Now starts collecting PHD immediately after you submit the configuration..

Configuring PHDC by Using the Service Now Devices Task

Junos Space Service Now allows you to configure PHD on a managed device from the Service Now Devices task after you assign the device to a product health data collection (PHDC) configuration. You can add the device to a PHDC configuration by creating a new configuration or to an existing PHDC configuration. A device can be added to an existing PHDC configuration only if the configuration is in the Scheduled or Running state. Once assigned to a PHDC configuration which is in Scheduled or Running state, you cannot assign the device to any other PHDC configuration.

> **NOTE:** PHDC consumes CPU cycles and disk resources of a device. Therefore, performance might be affected while PHD is being collected from the device.

To configure PHD collection on a device:

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

   The Service Now Devices page appears.

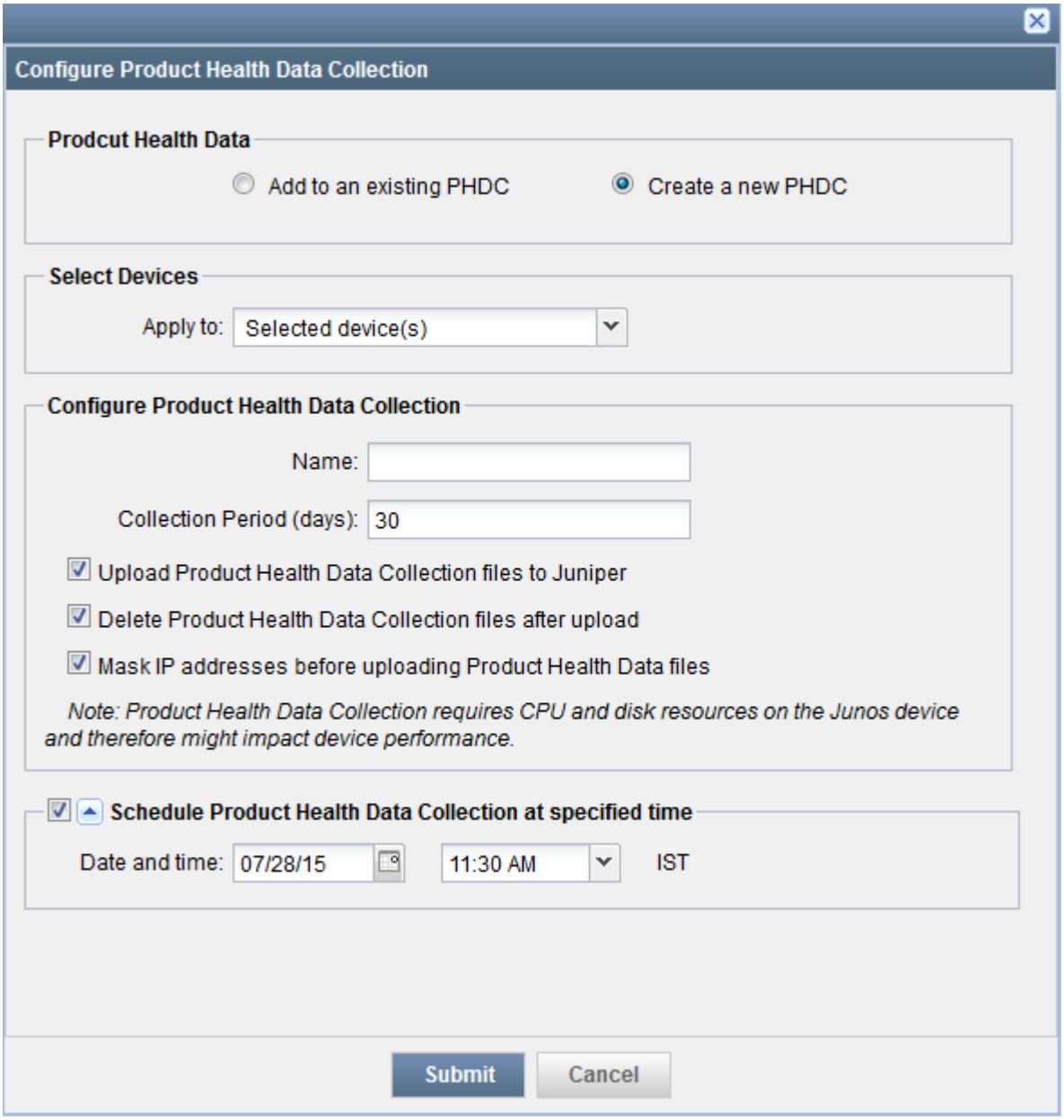
2. Select one or more devices to configure PHDC.

   > **NOTE:** PHDC can be configured on a maximum of 500 devices at a time.

3. From the Actions list , select **Device Analysis > Configure Product Health Data Collection**. Alternatively, right-click the selected devices and select **Device Analysis > Configure Product Health Data Collection**.

   The Configure Product Health Data Collection dialog box appears as show in Figure 72 on page 304.

Figure 72: Configure Product Health Data Collection Dialog Box



4. On the Configure Product Health Data Collection dialog box, add devices to an existing or new PHDC configuration as follows:

   - Add the selected devices to an existing PHDC configuration.

To add the selected devices to an existing PHDC configuration:

a. Click **Add to an existing PHDC**.

   An option to select a PHDC configuration for assigning the selected devices appear.

b. Select a PHDC configuration from the **PHDC** drop-down list to add the device.

- Add the selected devices to a new PHDC configuration.

  To add the selected devices to a new PHDC configuration:

  a. Click **Create a new PHDC**.

     Options to configure a new PHDC appear.

  b. From the **Apply to** drop-down list, select one of the following:

     - **Selected device(s)** to configure PHD collection on all devices selected on the Service Now Devices page
     - **All devices in the current domain** to configure PHD collection on all managed devices in the domain in which you are logged in
     - **Select Tag** to configure PHD collection on devices having a specific tag

       The Select from available Tags drop-down list appears when you select the Select tag option. Select a tag from the **Select from available Tags** drop-down list.

     - **Select Device Group** to configure PHD collection on devices belonging to a specific device group

       The Select from available Device Groups drop-down list appears when you select the Select Device Group option. Select a device group from the **Select from available Device Groups** drop-down list.

  c. Under Configure Product Health Data Collection, configure options as follows:

     - **Name**: Enter a name for the PHDC configuration.

       The name of a PHDC configuration must have 4 to 64 alphanumeric characters. Underscore(_) and hyphen (-) are the only special characters allowed.

     - **Collection Period (days)**: Enter the number of days when Service Now should collect product health data (PHD) from the devices.

       Number of days can range from 1 to 90. The default value is 30 days.

     - **Upload Product Health Data files to Juniper**: Select this check box if you want Service Now to upload PHD files collected from devices to Juniper Support Systems (JSS) or Service Now partner.

       This option is selected by default.

> **NOTE:** If you clear this check box, PHD files are not uploaded to JSS. If required later, you cannot upload PHD files to JSS.

- **Delete Product Health Data files after upload**: Select this check box to delete PHD files from Service Now immediately after they are uploaded to JSS.

  This option is selected by default.

> **NOTE:** If you clear this check box, PHD files are automatically deleted four days after the files are collected by Service Now.

- **Mask IP addresses before uploading Product Health Data files**: Select this check box if you want Service Now to replace IP addresses with asterisks (*) in the collected PHD.

  This option is selected by default.

- (Optional) **Schedule PHD Collection at specified time**: Select this check box to schedule a date and time for collecting PHD from the selected devices.

5. Click **Submit** to save the PHDC configuration.

   If Service Now configures PHDC successfully, you can view the configuration on the Product Health Data Collection page (**Administration > Product Health Data Collection**).

   If a time is scheduled, Service Now initiates PHD collection at the scheduled time. If a time is not scheduled, Service Now starts collecting PHD immediately after PHDC is configured.

RELATED DOCUMENTATION

- Product Health Data Collection Configuration Overview | 297
- Modifying a Product Health Data Collection Configuration | 310
- Rescheduling a Product Health Data Collection Configuration | 313
- Retrying Collecting Product Health Data from a Device | 315
- Disabling Product Health Data Collection on a Device | 316
- Enabling Product Health Data Collection on a Device | 317
- Aborting a Product Health Data Collection Configuration | 319
- Exporting Product Health Data Information to an Excel File | 321

Viewing Product Health Data Files Collected from a Device

Junos Space Service Now stores product health data (PHD) as PHD files in the Service Now database. Service Now uploads these files to Juniper Support Systems (JSS) for assessment. You can view the list of PHD files collected for a device on theView all Product Health Data Files page as shown in Figure 73 on page 307. You can also download, export, and delete the PHD files by using this page.

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

Figure 73: View All Product Health Data Files Page

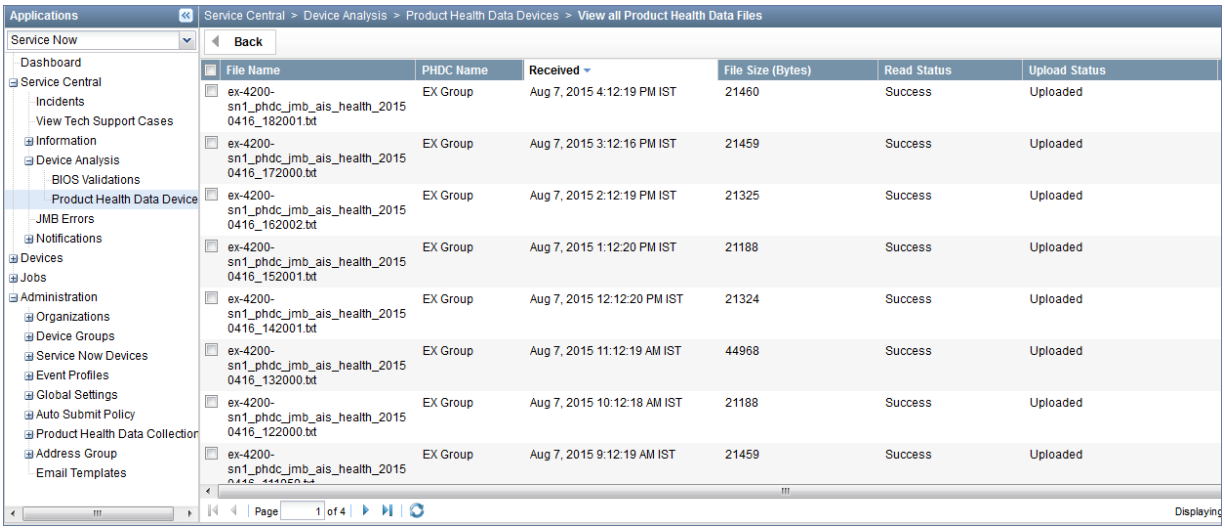


Table 26: Fields on the View All Product Health Data Files Page

Field Name	Description
File Name	Name of the PHD file The name is specified in the following format: *hostname*-sys_phdc_jmb_ais_health_*yyyymmdd_hhmmss*,where • *hostname* is the hostname of the device from which PHD is collected. • *yyyymmdd* is the date when PHD was collected. • *hhmmss* is the time when PHD was collected.
PHDC Name	PHDC configuration used to collect PHD

Table 26: Fields on the View All Product Health Data Files Page *(continued)*

Field Name	Description
Received	Date and time when Service Now collected PHD
File Size (Bytes)	Size of the PHD file in bytes
Read Status	Read status of PHD from the device Possible values: • Not Received—Service Now has not yet collected PHD from the device. • Success—Service Now has successfully collected PHD from the device. • Failure—Service Now failed to collect PHD from the device. • No Longer Available— PHD is no longer available on the device. • Successfully Deleted—PHD is successfully deleted from the device after it is collected by Service Now. • Reading from Device—Service Now is currently reading PHD from the device. • Read Complete—Service Now has completed reading PHD from the device. • Processing—Service Now is processing PHD to create the PHD files.
Upload Status	Status of uploading PHD files to JSS: • Not Uploaded—Service Now has not yet uploaded PHD files to JSS. • Success—Service Now has successfully uploaded PHD files to JSS. • Failure—Upload of PHD files to JSS failed. • Uploading—Service Now is uploading PHD files to JSS.
Remarks	Remarks about a failed condition such as failure to read PHD from the device or upload a PHD file to JSS

To view the PHD files collected from a device:

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

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

      The Product Health Data Devices page appears.

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

      The View All Product Health Data Files page appears.

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

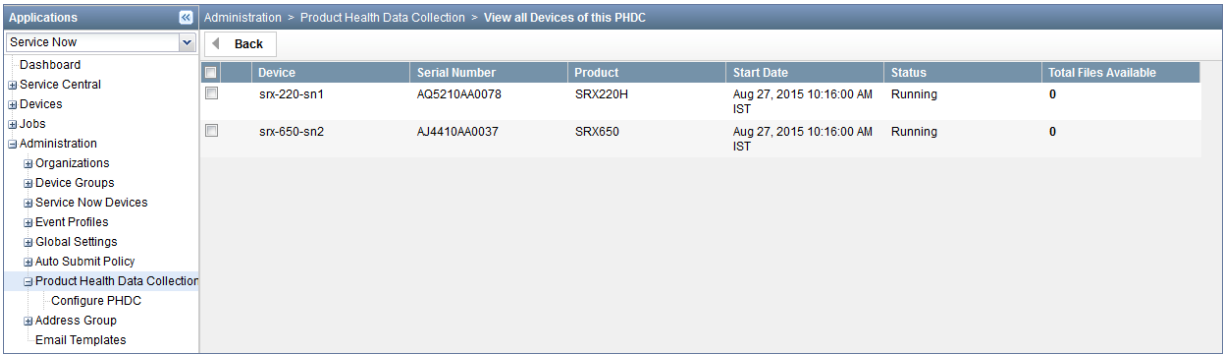
   a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

      The Product Health Data Collection page appears.

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

      The View All Devices of this PHDC page appears as shown in Figure 74 on page 309. The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 74: View All Devices of this PHDC Page



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

      The View All Product Health Data Files page appears.

2. On the View All Product Health Data Files page, click one or more files that you want to select for download.

3. Right-click the selection and select **Download Product Health Data File**.

   The Download Product Health Data Files dialog box appears.

4. Click the **Download** button.

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

5. Click the **Download** link.

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

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

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

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

RELATED DOCUMENTATION

Service Now Product Health Data Collection Overview

Product Health Data Collection Configuration Overview | 297

Exporting Product Health Data Information to an Excel File | 321

Deleting Product Health Data Files Collected from a Device | 327

Deleting a Product Health Data Collection Configuration from Service Now | 329

Modifying a Product Health Data Collection Configuration

The parameters of a PHDC configuration that you can modify depend on the state of the PHDC configuration. You cannot modify the name of a PHDC configuration.

You can modify the following parameters of a PHDC configuration:

- Devices assigned to PHDC

  Devices can be assigned and deleted from a PHDC configuration if the PHDC configuration status is not Aborted.

  When you assign a device to a PHDC configuration in the Running state, product health data (PHD) is collected from the device for the number of days that are remaining in the configuration. For example, if you assign a device to a PHDC configuration, that is, in running state and configured to run for 10 days, on the fourth day of PHD collection, PHD is collected from the device for the remaining six days.

- Collection period

  PHD collection period can be changed if the PHDC configuration status is not Aborted.

  To extend the number of days of PHD collection, the number of days to be extended should be added to the collection period currently configured. For example, to extend PHD collection period of 30 days by ten days, enter 40 (30 + 10) for the Collection period.

  To reduce the number of days of PHD collection, the number of days to be reduced should be removed from the collection period currently configured. For example, to reduce the collection period by 10 days, enter 20 (30 - 10) as the Collection period. If you are modifying the collection period 20 days after the PHD collection started (say on the 22nd day or 23rd day, the PHD collection is stopped on the devices.

- Upload Product Health Data Files to Juniper

  The option to upload PHD files to JSS can be changed only when the status of a PHDC configuration is Scheduled.

- Delete PHD files after upload

  The option to delete PHD files from Service Now after upload to JSS can be changed only when the status of a PHDC configuration is Scheduled.

- Mask IP address before uploading PHD files

  The option to mask IP address in the PHD files before uploading the files to JSS can be changed only when the status of a PHDC configuration is Scheduled.

To modify a PHDC configuration:

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

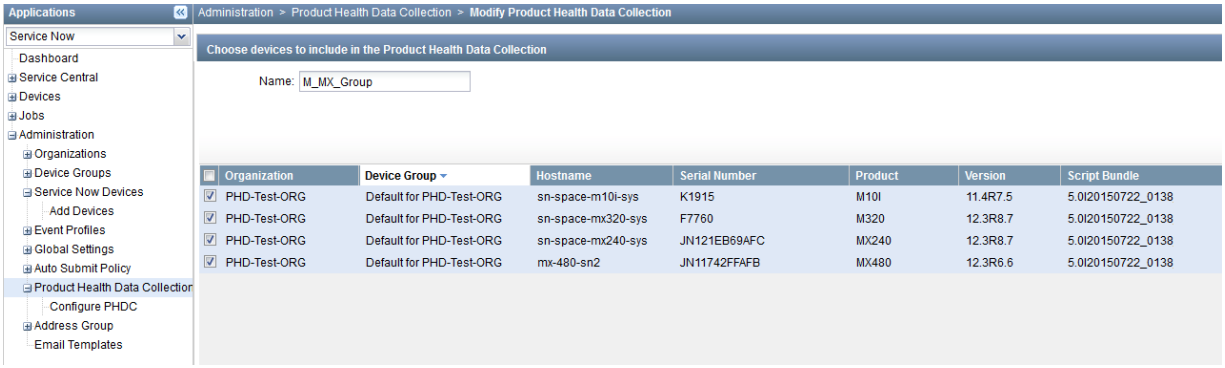
   The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, select the PHDC configuration that you want to modify.

3. From the Actions list, select **Modify Product Health Data Collection group**. Alternatively, right-click the PHDC configuration and select **Modify Product Health Data Collection** .

   The Modify Product Health Data Collection page appears as shown in Figure 75 on page 312.

Figure 75: Modify Product Health Data Collection Page



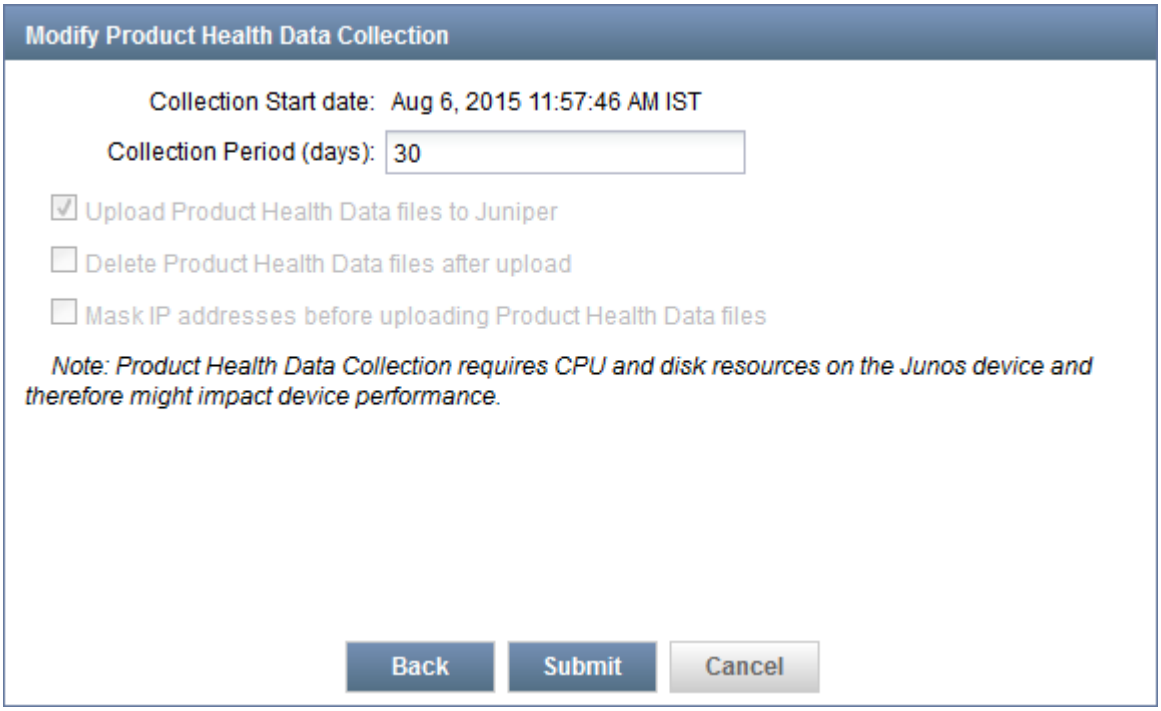
4. (Optional) Click the **Show Selected Devices** link to view the devices included in the PHDC configuration.

5. Add or remove one or more devices from the PHDC configuration by selecting or clearing the check boxes provided next to the devices.

6. Click **Next**.

   Service now displays the Modify Product Health Data Collection page.

Figure 76: Modify Product Health Data Collection Parameters



7. Modify **Collection Period (days)**.

The PHD Collection Period can vary from 1 to 90 days.

8. If the PHDC configuration is in Scheduled state, you can modify the following parameters:
   - **Upload Product Health Data files to Juniper**
   - **Delete Product Health Data files after upload**
   - **Mask IP addresses before uploading Product Health Data files**
9. Click **Submit**.

   Service Now displays a message indicating the PHDC configuration is successfully modified..

RELATED DOCUMENTATION

- Aborting a Product Health Data Collection Configuration | 319
- Disabling Product Health Data Collection on a Device | 316
- Retrying Collecting Product Health Data from a Device | 315
- Rescheduling a Product Health Data Collection Configuration | 313
- Configuring Product Health Data Collection on a Device | 300
- Viewing Product Health Data Files Collected from a Device | 307
- Product Health Data Collection Configuration Overview | 297
- Configuring Product Health Data Collection on a Device | 300

Rescheduling a Product Health Data Collection Configuration

You can reschedule a product health data collection (PHDC) configuration if the PHDC status of the configuration is Completed. See "Product Health Data Collection Configuration Overview" on page 297 for details on the status of PHDC configuration.

When you reschedule a PHDC configuration, the *Copy of* prefix is added to the name of the PHDC configuration. While rescheduling, you can add or remove devices from the configuration and modify the PHD collection period.

To reschedule a PHDC configuration:

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

   The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, select the PHDC configuration that you want to reschedule.

3. From the Actions list, select **Reschedule**. Alternatively, right-click the PHDC configuration and select **Reschedule**.

   The Reschedule page appears.

4. (Optional) Select or remove devices from the PHDC configuration by selecting or clearing the check boxes provided next to the devices.

5. Click **Next**.

   The Configure Product Health Data Collection parameters appear.

6. (Optional) Modify the **Collection Period (days)**.

7. (Optional) Select a schedule date and time to start the PHD collection.

8. Click **Submit** to reschedule PHDC or click **Cancel** to cancel rescheduling PHDC.

   When you click Submit, Service Now displays a message indicating that PHDC configuration is successfully rescheduled. If a date and time is not scheduled for PHD collection, Service Now starts collecting PHD immediately after you submit the configuration and changes the status of the PHDC configuration to Starting and then Running.

RELATED DOCUMENTATION

- Product Health Data Collection Configuration Overview | **297**
- Configuring Product Health Data Collection on a Device | **300**
- Aborting a Product Health Data Collection Configuration | **319**
- Disabling Product Health Data Collection on a Device | **316**
- Retrying Collecting Product Health Data from a Device | **315**
- Modifying a Product Health Data Collection Configuration | **310**
- Viewing Product Health Data Files Collected from a Device | **307**

Retrying Collecting Product Health Data from a Device

You can retry collecting product health data (PHD) on a device assigned to a product health data collection (PHDC) configuration if an earlier attempt to collect PHD from the device failed (that is, the PHD collection status of the device is Failed) and if the status of PHDC configuration is Running. See *Service Now Product Health Data Collection Overview* for details about the statuses of PHD collection on a device and "Product Health Data Collection Configuration Overview" on page 297 for details about the statuses of PHDC configuration.

To retry collecting PHD from a device on which PHD collection failed:

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

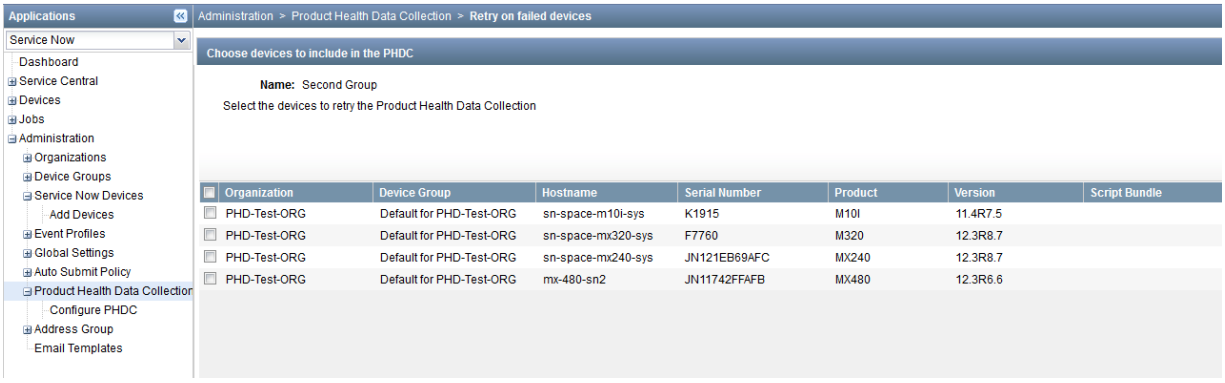
   The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, select the PHDC configuration assigned to the device on which you want to retry collecting PHD.

3. From the Actions list, select **Retry on failed devices**. Alternatively, right-click the PHDC configuration and select **Retry on failed devices**.

   The Retry on failed devices page appears as shown in Figure 77 on page 315. The page lists the devices in the configuration on which an earlier attempt to collect PHD failed.

Figure 77: Retry on Failed Devices Page



4. In the table, click the devices on which you want to retry PHD collection.

5. Click **Submit** to retry PHD collection or click **Cancel** to cancel retrying PHD collection.

   When you click Submit, Service Now displays a message indicating that the PHD collection is attempted again on selected devices. The PHD collection status for the devices is changed to Scheduled, Starting and then Running if the retry is successful.

RELATED DOCUMENTATION

- Product Health Data Collection Configuration Overview | 297
- Configuring Product Health Data Collection on a Device | 300
- Aborting a Product Health Data Collection Configuration | 319
- Disabling Product Health Data Collection on a Device | 316
- Rescheduling a Product Health Data Collection Configuration | 313
- Modifying a Product Health Data Collection Configuration | 310
- Viewing Product Health Data Files Collected from a Device | 307

Disabling Product Health Data Collection on a Device

Product health data (PHD) collection can be disabled on any device assigned to a PHDC configuration if the PHD collection status of the device is Running or Enabled and the status of the PHDC configuration is Running. The Disable option allows you to disable PHD collection selectively on devices in a PHDC configuration without affecting the PHD collection on other devices.

To disable PHD collection on a device:

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

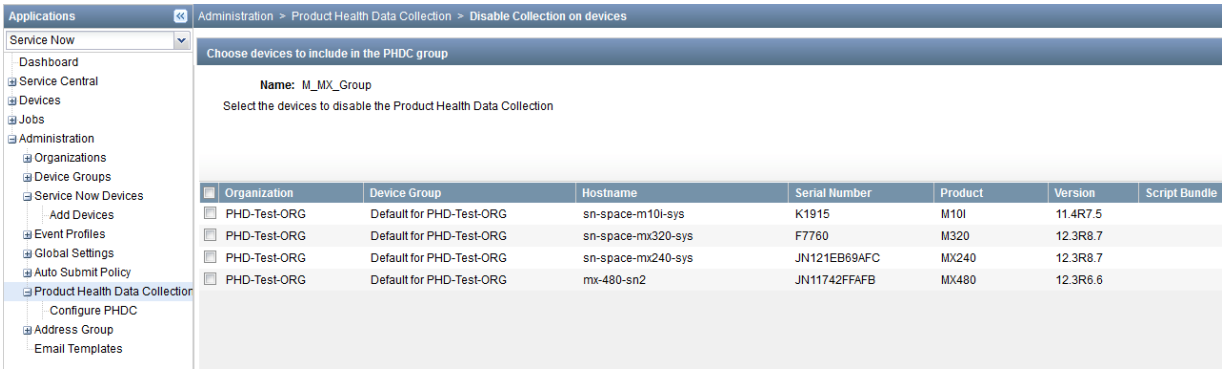
   The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, click the PHDC configuration in which you want to disable PHDC on one or more devices.

3. From the Actions list, select **Disable Collection on devices**. Alternatively, right-click the PHDC configuration and select **Disable Collection on devices**.

   The Disable Collection on devices page appears as shown in Figure 78 on page 317. The page lists the devices on which PHD collection can be disabled.

Figure 78: Disable Collection on Devices Page



4. In the table, select the devices on which you want to disable PHD collection.

5. Click **Submit** to disable PHD collection on selected devices or click **Cancel** to cancel disabling PHD collection.

   On clicking Submit, Service Now displays a message indicating that the PHD collection is disabled on selected devices and the PHD collection status for the devices is changed to disabled.

RELATED DOCUMENTATION

- Product Health Data Collection Configuration Overview | 297
- Configuring Product Health Data Collection on a Device | 300
- Aborting a Product Health Data Collection Configuration | 319
- Retrying Collecting Product Health Data from a Device | 315
- Rescheduling a Product Health Data Collection Configuration | 313
- Modifying a Product Health Data Collection Configuration | 310
- Viewing Product Health Data Files Collected from a Device | 307

Enabling Product Health Data Collection on a Device

Product health data (PHD) collection can be enabled on devices of a PHDC configuration if PHD collection was earlier disabled on the devices. This option allows you to enable PHD collection selectively on a device in a PHDC configuration without affecting the disabled status of PHD collection on other devices.

To enable PHD collection on a device of a PHDC configuration:

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

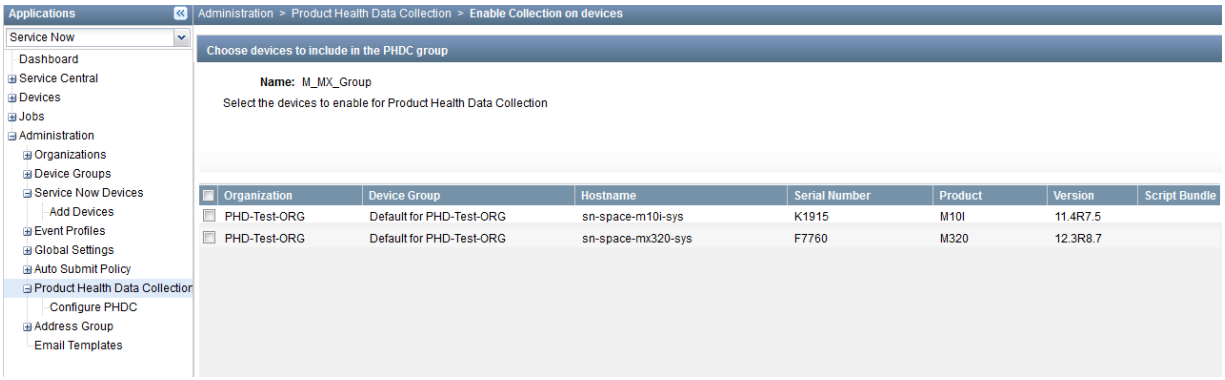
   The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, click the PHDC configuration to which the device on which you want to enable PHD collection is assigned.

3. From the Actions list, select **Enable Collection on devices**. Alternatively, right-click the PHDC configuration and select **Enable Collection on devices**.

   The Enable Collection on Devices page appears as shown in Figure 79 on page 318. The page lists the devices on which PHDC can be enabled.

Figure 79: Enable Collection on Devices Page



4. In the table, click the devices on which you want to enable PHD collection.

5. (Optional) Click the **Show Selected Devices** link to view the devices selected for enabling PHDC.

   Click **Close** to return back to the Enable Collection on Devices page.

6. Click **Submit** to enable PHD collection on selected devices or click **Cancel** to cancel enabling PHD collection.

   On clicking Submit, Service Now displays a message indicating PHD collection is enabled on selected devices and the PHD collection status for the device is changed to enabled.

RELATED DOCUMENTATION

Product Health Data Collection Configuration Overview | 297

Configuring Product Health Data Collection on a Device | 300
Aborting a Product Health Data Collection Configuration | 319
Retrying Collecting Product Health Data from a Device | 315
Rescheduling a Product Health Data Collection Configuration | 313
Modifying a Product Health Data Collection Configuration | 310
Viewing Product Health Data Files Collected from a Device | 307

Aborting a Product Health Data Collection Configuration

You can abort product health data collection (PHDC) configuration when the status of PHDC is Running. This action aborts PHD collection on all devices assigned to the PHDC configuration.

> **NOTE:** Once you abort a PHDC configuration, you can only delete the configuration. You cannot move it to any other state.

To abort PHDC configuration:

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

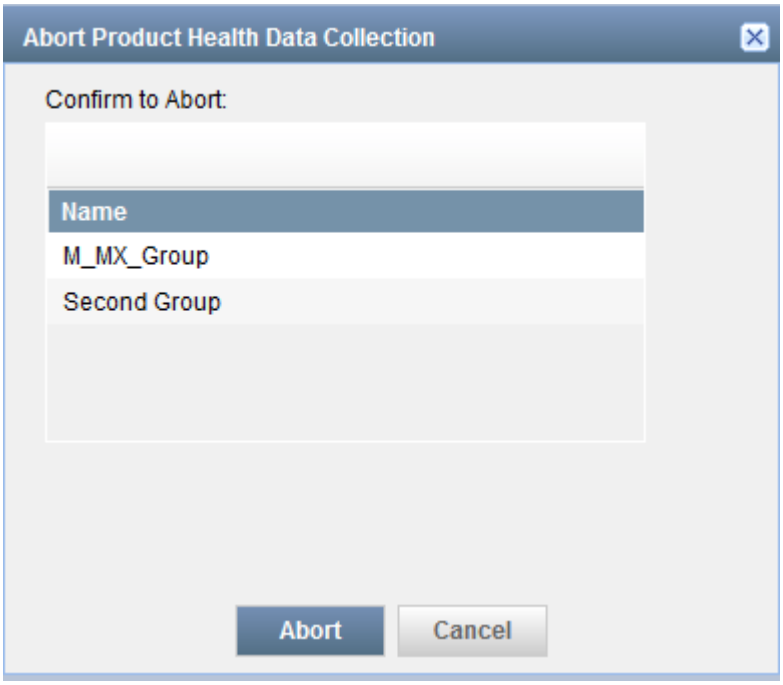
   The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, select one or more PHDC configurations that you want to abort.

3. From the Actions list, select **Abort**. Alternatively, right-click the PHDC configuration and select **Abort**.

   The Abort Product Health Data Collection dialog box is displayed as shown in Figure 80 on page 320.

Figure 80: Abort Product Health Data Collection Dialog Box



4. Click **Abort** to abort the PHDC configuration or click **Cancel** to cancel aborting.

   On clicking Submit, Service Now displays a message indicating that the PHDC configuration is successfully aborted and sets the status of the PHDC configuration and the PHD collection to aborted.

RELATED DOCUMENTATION

- Product Health Data Collection Configuration Overview | 297
- Configuring Product Health Data Collection on a Device | 300
- Disabling Product Health Data Collection on a Device | 316
- Enabling Product Health Data Collection on a Device | 317
- Retrying Collecting Product Health Data from a Device | 315
- Rescheduling a Product Health Data Collection Configuration | 313
- Modifying a Product Health Data Collection Configuration | 310
- Viewing Product Health Data Files Collected from a Device | 307

Exporting Product Health Data Information to an Excel File

IN THIS SECTION

- Exporting Information about Devices on which PHDC is configured | 322
- Exporting Data about PHD Files Collected from a Device | 324

Junos Space Service Now provides the Export and Export All options in the Actions list of the Product Health Data Devices page to export the following information in an Excel file:

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

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

  Figure 81 on page 321 shows a sample of the information about devices exported to Excel.

Figure 81: PHDC Information of Devices Exported to Excel

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

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

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

  Figure 82 on page 322 shows a sample of the information about PHD files exported to Excel.

Figure 82: PHD Files Information Exported to Excel

	A	B	C	D	E	F	G
1							
2	**Device Name**	mx-480-sn1					
3	**Total Number of PHD**	25					
4							
5	**File Name**	**Group Name**	**Size (Bytes)**	**Received (UTC)**	**Read Status**	**Upload Status**	**Remarks**
6							
7	mx-480-sn1_phdc_jmb_	Test-group	59548	2015-07-16 10:18:08.19	Success	Success	
8	mx-480-sn1_phdc_jmb_	Test-group	59984	2015-07-16 23:18:06.51	Success	Not Uploaded	
9	mx-480-sn1_phdc_jmb_	Test-group	N/A	2015-07-17 02:19:22.55	Not Received	Not Uploaded	
10	mx-480-sn1_phdc_jmb_	Test-group	59561	2015-07-16 13:18:03.25	Success	Success	
11	mx-480-sn1_phdc_jmb_	Test-group	90203	2015-07-16 02:19:16.46	Success	Success	
12	mx-480-sn1_phdc_jmb_	Test-group	59552	2015-07-16 05:18:07.90	Success	Success	
13	mx-480-sn1_phdc_jmb_	Test-group	59758	2015-07-16 16:18:03.51	Success	Success	
14	mx-480-sn1_phdc_jmb_	Test-group	59561	2015-07-16 19:18:08.45	Success	Not Uploaded	
15	mx-480-sn1_phdc_jmb_	Test-group	59416	2015-07-16 06:18:01.12	Success	Success	
16	mx-480-sn1_phdc_jmb_	Test-group	59832	2015-07-16 22:18:06.82	Success	Not Uploaded	
17	mx-480-sn1_phdc_jmb_	Test-group	59812	2015-07-16 09:18:03.65	Success	Success	
18	mx-480-sn1_phdc_jmb_	Test-group	59569	2015-07-17 01:18:07.51	Success	Not Uploaded	
19	mx-480-sn1_phdc_jmb_	Test-group	59556	2015-07-16 12:18:03.29	Success	Success	
20	mx-480-sn1_phdc_jmb_	Test-group	59563	2015-07-16 15:18:10.06	Success	Success	
21	mx-480-sn1_phdc_jmb_	Test-group	59949	2015-07-16 03:18:01.24	Success	Success	

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

Exporting Information about Devices on which PHDC is configured

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

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

1. • To export the information from the Product Health Data Devices task:

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

      The Product Health Data Devices page appears.

   • To export the PHD files from the Product Health Data Collection task:

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

      The Product Health Data Collection page appears.

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

      The View all Devices of this PHDC page appears as shown in Figure 83 on page 323. The View all Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 83: View all Devices of this PHDC

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

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

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

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

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

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

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

Exporting Data about PHD Files Collected from a Device

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

To export data about PHD files collected from a device:

1. • To export the PHD files from the Product Health Data Devices task:

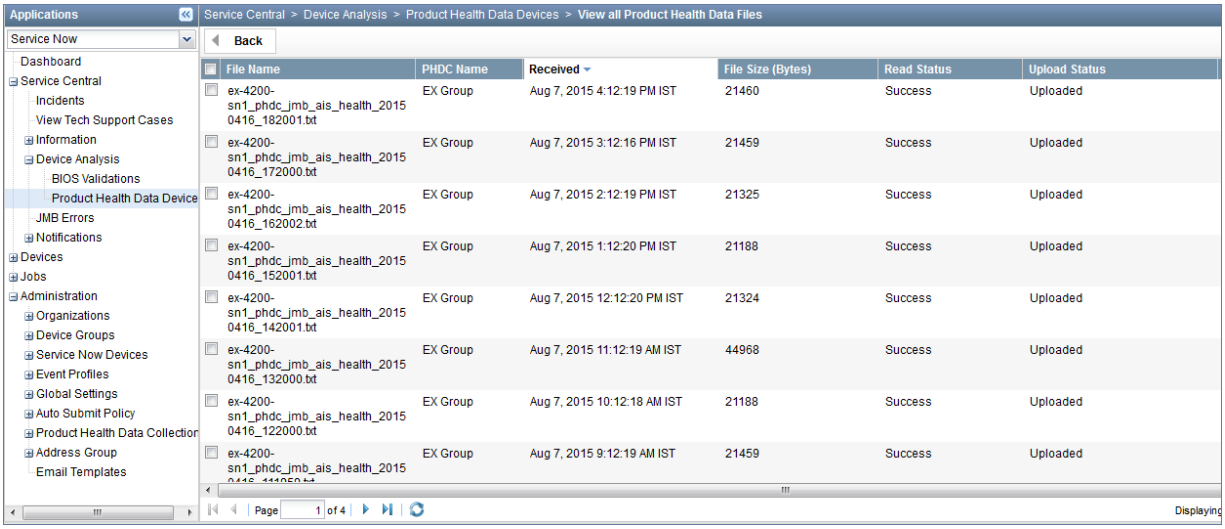
   a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

      The Product Health Data Devices page appears.

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

      The View All Product Health Data Files page appears as shown in Figure 84 on page 325.

Figure 84: View All Product Health Data Files Page



- To export the PHD files from the Product Health Data Collection task:

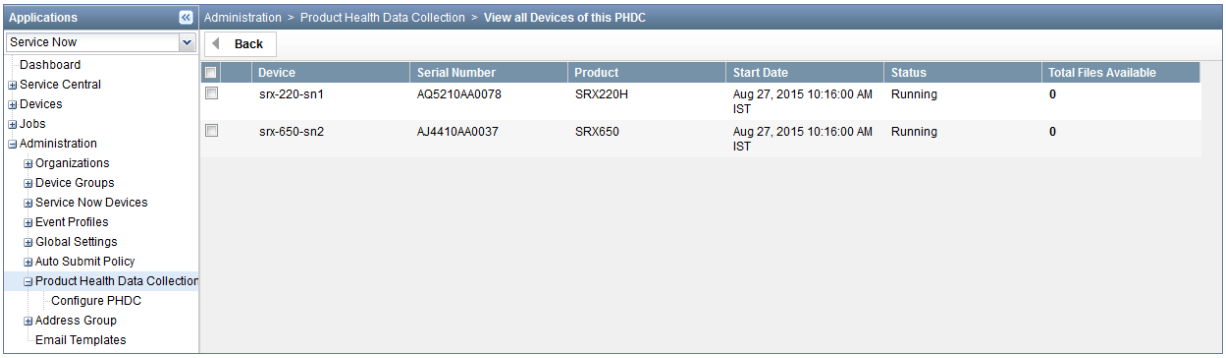
  a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

     The Product Health Data Collection page appears.

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

     The View All Devices of this PHDC page appears as shown in Figure 85 on page 325. The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 85: View All Devices of this PHDC Page



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

   The View all Product Health Data Files page appears.

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

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

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

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

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

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

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

RELATED DOCUMENTATION

Service Now Product Health Data Collection Overview

Viewing Product Health Data Files Collected from a Device | 307

Product Health Data Collection Configuration Overview | 297

Deleting Product Health Data Files Collected from a Device

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

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

To delete the PHD files collected from a device:

1. • To delete the PHD files from the Product Health Data Devices task of the Service Central workspace:

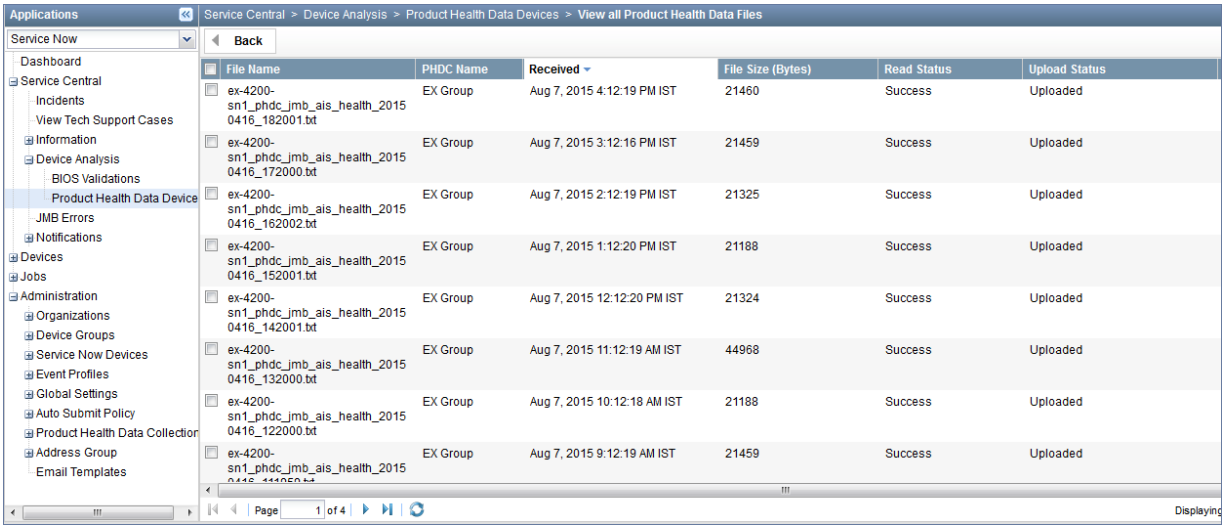
   a. From the Service Now navigation tree, select **Service Central > Device Analysis > Product Health Data Devices**.

      The Product Health Data Devices page appears.

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

      The View All Product Health Data Files page appears as shown in Figure 86 on page 327.

Figure 86: View All Product Health Data Files Page



• To delete the PHD files from the Product Health Data Collection task of the Administration workspace:

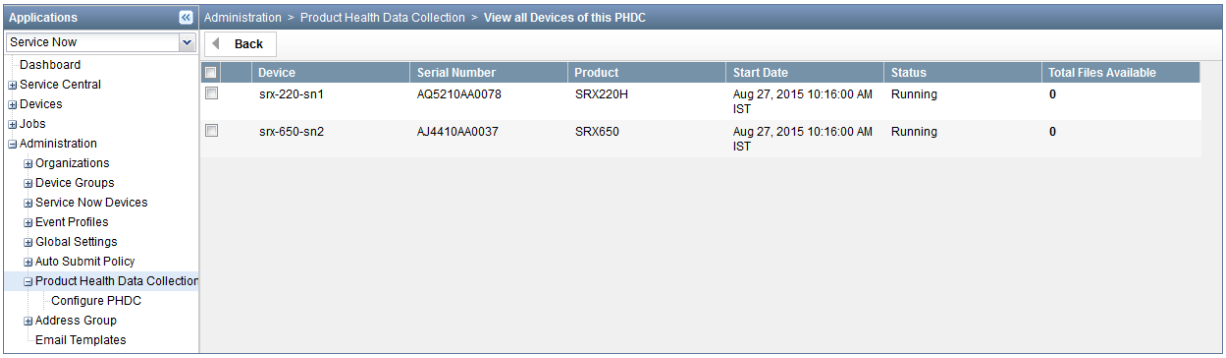
a. From the Service Now navigation tree, select **Administration > Product Health Data Collection**.

   The Product Health Data Collection page appears.

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

   The View All Devices of this PHDC page appears as shown in Figure 87 on page 328. The View All Devices of this PHDC page displays the number of PHD files collected for each device assigned to the PHDC configuration.

Figure 87: View All Devices of this PHDC Page



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

   The View All Product Health Data Files page appears.

2. On the View All Product Health Data Files:

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

     The Delete Selected Product Health Data Files dialog box appears.

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

     The Delete All Product Health Data Files dialog box appears.

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

   If you click the Delete button, Service Now displays a message indicating that the files are deleted.

RELATED DOCUMENTATION

Service Now Product Health Data Collection Overview

Product Health Data Collection Configuration Overview | 297
Viewing Product Health Data Files Collected from a Device | 307
Exporting Product Health Data Information to an Excel File | 321

Deleting a Product Health Data Collection Configuration from Service Now

Service Now provides the Delete option on the Actions list to delete a PHDC configuration. You can delete a PHDC configuration if the status of the configuration is not Running.

To delete a PHDC configuration:

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

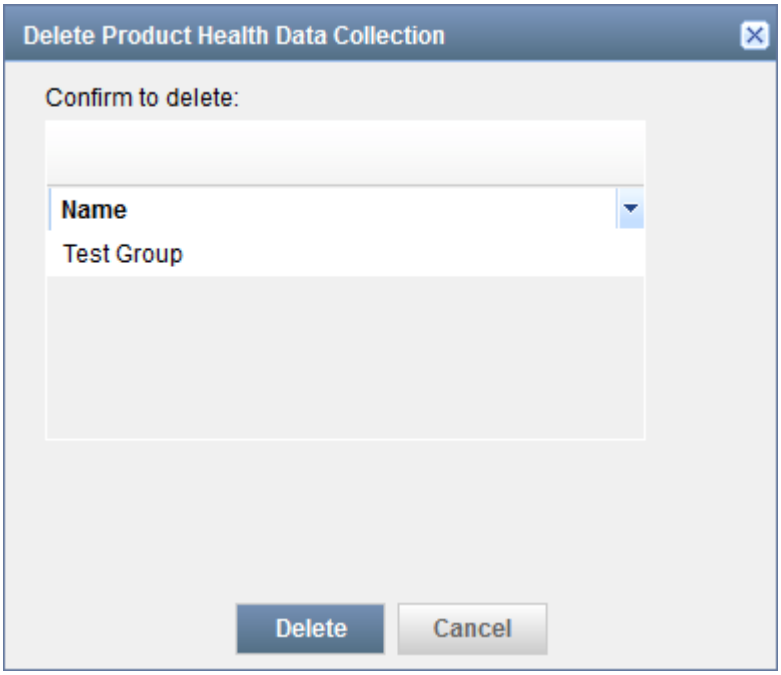
   The Product Health Data Collection page appears.

2. On the Product Health Data Collection page, select the PHDC configuration that you want to delete.

3. From the Actions list , select **Delete**. Alternatively, right-click the PHDC configuration and select **Delete**.

   The Delete Product Health Data Collection dialog box appears as shown in Figure 88 on page 330.

Figure 88: View all Product Health Data Files Page



4. Click **Delete** to delete the PHDC configuration or click **Cancel** to cancel the deletion.

   When you click Submit, Service Now displays a message indicating that the PHDC configuration is successfully deleted.

RELATED DOCUMENTATION

- Product Health Data Collection Configuration Overview | 297
- Configuring Product Health Data Collection on a Device | 300
- Viewing Product Health Data Files Collected from a Device | 307
- Disabling Product Health Data Collection on a Device | 316
- Enabling Product Health Data Collection on a Device | 317
- Retrying Collecting Product Health Data from a Device | 315
- Rescheduling a Product Health Data Collection Configuration | 313
- Modifying a Product Health Data Collection Configuration | 310

15

CHAPTER

Configuring and Managing Address Groups

Service Now Address Group Overview | **333**

Creating an Address Group | **334**

Modifying an Address Group | **334**

Deleting Address Groups | **335**

Associating Devices with an Address Group From the Address Groups Page | **336**

Associating Devices with an Address Group From the Organizations Page | **338**

Associating Devices with an Address Group from the Device Groups Page | **340**

Associating Devices with an Address Group from the Service Now Devices Page | **341**

Service Now Address Group Overview

Junos Space Service Now provides the Address Group task to configure addresses where devices are located and assign those addresses to devices. This address is used by Juniper Networks for shipping replacement parts and mail communications. You can view address groups configured on Service Now on the Address Groups page (**Administration > Address Group)**.

A Service Now partner can use the partner address instead of end-customer address when submitting RMA cases for end customers to Juniper Support Systems (JSS). This can be done through a setting at the connected member and when submitting a case manually. For an auto submit policy, the partner address can be used if this feature is selected by the partner. Otherwise the end-customer address is used. If the partner uses the partner address, both partner address and customer address must be shown for the device. However, only the partner address is shown when submitting an incident to Juniper Networks.

You can associate devices to any of the address groups defined in the system. You can also associate devices to address group subtypes (Location, Ship- to, and Both) from the Organizations page, Device Groups page, and Devices page.

Associated Actions

You can perform the following actions related to address groups:

- View address groups configured in Service Now
- Create a new address group; see “Creating an Address Group” on page 334 for details.
- Modify an existing address group; see “Modifying an Address Group” on page 334 for details.
- Delete address groups; see “Deleting Address Groups” on page 335 for details.
- Associate address group to a set of devices; see “Associating Devices with an Address Group From the Address Groups Page” on page 336 for details.

RELATED DOCUMENTATION

Service Now Devices Overview | **147**

Service Now Organizations Overview | **119**

Service Now Device Groups Overview | **137**

Generating an RMA Incident for a Device | **182**

Creating an Address Group

To create an address group:

1. From the Service Now navigation tree, select **Administration** > **Create Address Group**.

   The Create Address Group page appears.

2. Enter data in the relevant fields.

   The Address Group name must be unique and can contain alphanumeric character, space, hyphen, and underscore. The maximum number of characters allowed is 255.

   Address Group Name, Address1, City and Country are mandatory fields.

3. Click **Submit**.

   Service Now creates the new address group and displays it on the Address Group page.

RELATED DOCUMENTATION

Service Now Address Group Overview | 333

Modifying an Address Group | 334

Deleting Address Groups | 335

Associating Devices with an Address Group From the Address Groups Page | 336

Modifying an Address Group

To modify an address group:

1. From the Service Now navigation tree, select **Administration** > **Address Group**.

   The Address Group page appears.

2. Select the address group that you need to modify, and select **Modify Address Group** from either the **Actions** list or the right-click menu. The Modify Address Group page appears.

3. Modify the relevant fields.

> **NOTE:** You cannot modify an address group name on this screen.

4. Select **Submit**.

   Service Now modifies the address group. You can view the modified address on the Address Group page.

RELATED DOCUMENTATION

- Service Now Address Group Overview | 333
- Creating an Address Group | 334
- Deleting Address Groups | 335
- Associating Devices with an Address Group From the Address Groups Page | 336

Deleting Address Groups

Junos Space Service Now provides the Delete option in the Actions list for the Address Groups page to delete address groups.

To delete address groups:

1. From the Service Now navigation tree, select **Administration** > **Address Group**. The Address Group page appears.

2. Select one or rmore address groups that you need to delete, and select **Delete** from either the **Actions** list or the right-click menu.

   The Delete Address Groups page appears.

3. Click **Delete** to delete the selected address groups.

   Service Now deletes the selected address groups and removes them from the Address Groups page.

RELATED DOCUMENTATION

- Service Now Address Group Overview | 333

Creating an Address Group | 334
Modifying an Address Group | 334
Associating Devices with an Address Group From the Address Groups Page | 336

Associating Devices with an Address Group From the Address Groups Page

Junos Space Service Now provides the Assoicate Devices option in the Actions list of the Address Groups page to associate devices with address groups.

To associate a device with an address group from the Address Groups page:

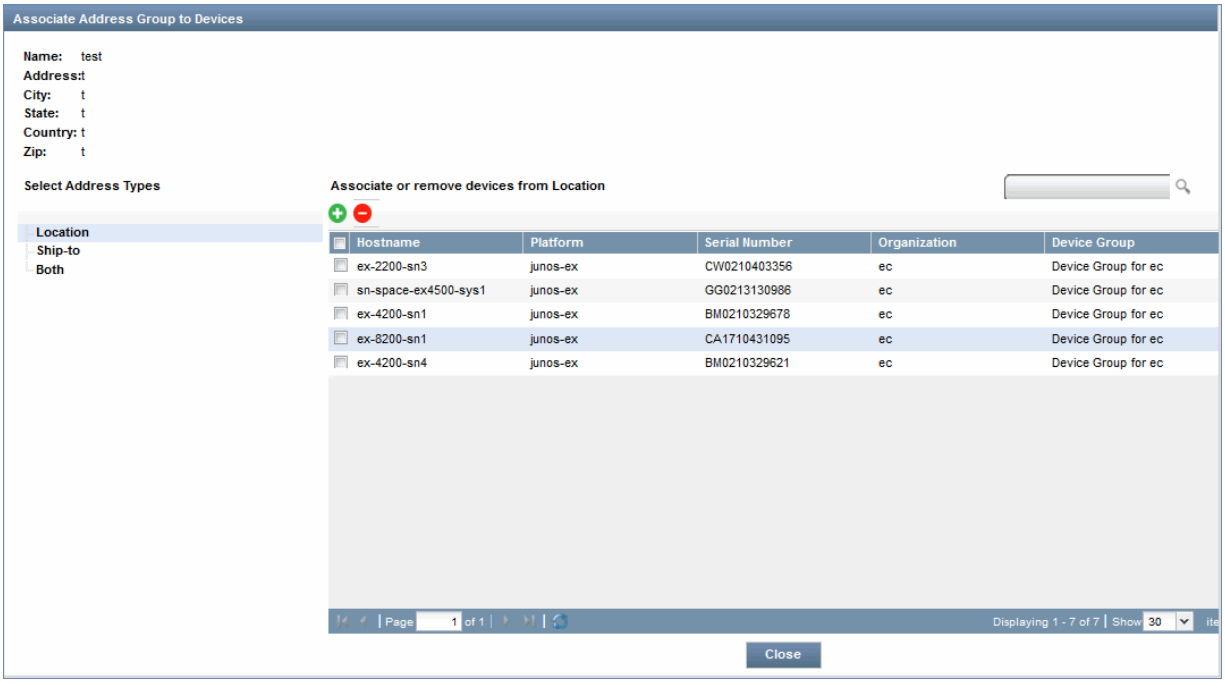
1. From the Service Now navigation tree, select **Administration** > **Address Group**.

   The Address Group page appears.

2. Select the address group that you want to associate with a device, and select **Associate Devices** from either the **Actions** list or the right-click menu.

   The Associate Address Group to Devices page appears as shown in Figure 89 on page 336.

Figure 89: Associate Address Group to Devices Page



You can associate devices to this address group in any of the following subtypes: Location, Ship-to or Both. These subtypes of the address group represent the device location or ship-to address of a device. In case of an RMA event, the ship-to address is used by logistics team of Juniper to ship the replacement of a defective part to the customer directly, without manual intervention. A device can have only one location or ship-to address associated to it. You can click **Location** to associate a device to a location. Repeat the same procedure for Ship-to and Both. Clicking on the left hand side menu alone results in displaying the already associated devices for this subtype. If you associate a device to both Ship-to and Location on an address group, all the previous associated links to the device are removed and the latest changes are effective.

You can assign an address to a device as its location, ship-to or both. In case of an RMA event, the ship-to address is used by the logistics team of Juniper to ship the defective parts for the device. A device can have only one location and ship-to address.

3. The address group must be assigned to the devices as the address of their location, shipping address or the address for both the location and shipping.
   - To assign the address group as the address of a device location, under **Select Address Types**, click **Location**.
   - To assign the address group as the shipping address for a device, under **Select Address Types**, click **Ship-to**.
   - To assign the address group as the address for both shipping and location, under **Select Address Types**, click **Both**.
4. In the **Associate or remove devices from** section, click the Plus icon.

   The Select Devices page appears listing all the devices present in service now. If required, filter the devices.
   - To filter by organization, in the **Show** list, select By Organization and select the Organization from the **Organization** list.
   - To filter by Device Group, in the **Show** list, select By Device Group and select the Device Group from the **Device Group** list
   - To filter by name of device, in the search field, enter the first few characters of the device name
5. Select the devices from the device list to assign the address group and click **Submit**.

   Service Now assigns the address configured in the address group to the selected devices' as the location, shipping address or the address for both shipping and location as specified in Step 3. and the Associate Address Group to Devices page is displayed.

6. To remove a device association from one of the subtypes, click on the subtype link on the left. The devices associated to the selected subtype are listed. Select a list of devices on the right and then click on the cross button on the right.

7. The Disassociate Devices window appears. Click **Remove**. The devices are removed from this address group subtype (Location, Ship-to or Both).

   Devices can also be associated to an address group sub types through organization page, device group page, and device page.

RELATED DOCUMENTATION

- Service Now Address Group Overview | 333
- Creating an Address Group | 334
- Modifying an Address Group | 334
- Deleting Address Groups | 335
- Associating Devices with an Address Group From the Organizations Page | 338
- Associating Devices with an Address Group from the Device Groups Page | 340
- Associating Devices with an Address Group from the Service Now Devices Page | 341

Associating Devices with an Address Group From the Organizations Page

Using Service Now, you can associate devices to address groups from the Organizations page.

To associate a device to an address group from the Organizations page:

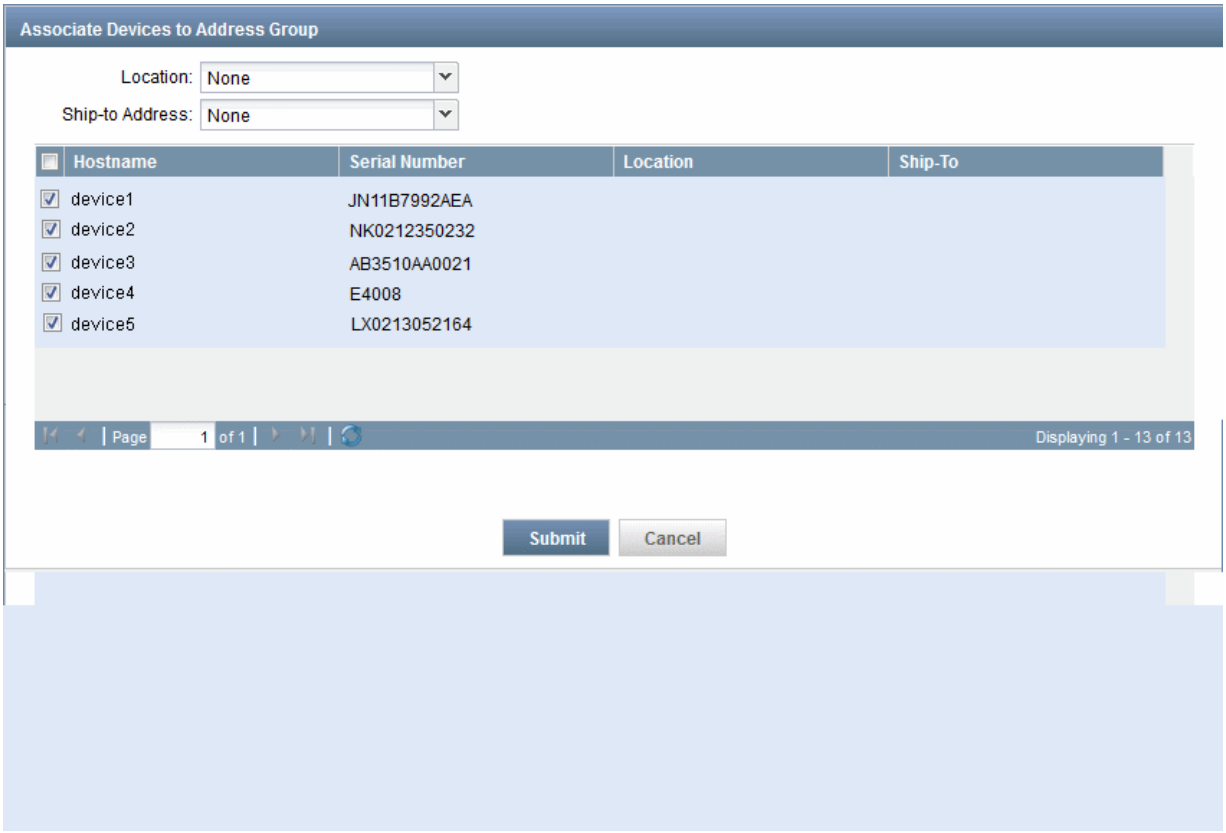
1. From the Service Now navigation tree, select **Administration** > **Organizations**.

   The Organizations page appears.

2. Select the address group that needs to be associated with a device, and select **Associate Address Group** from either the **Actions** list or the right-click menu.

   The Associate Devices to Address Group page appears.

Figure 90: Associate Devices to Address Group Page



3. Select the address group/Address group subtype [i.e. Location and Ship to Address] from the combo box and click **Submit**.

   All the selected devices are associated to the new address group/address subtype. This page lists the devices present under the selected organization. The Location and Ship-to Address fields show address group names if the devices already have an association present in the system

RELATED DOCUMENTATION

Service Now Organizations Overview | **119**

Associating Devices with an Address Group From the Address Groups Page | **336**

Associating Devices with an Address Group from the Device Groups Page | **340**

Associating Devices with an Address Group from the Service Now Devices Page | **341**

Associating Devices with an Address Group from the Device Groups Page

Using Service Now, you can associate devices to address groups from the Device Groups page.

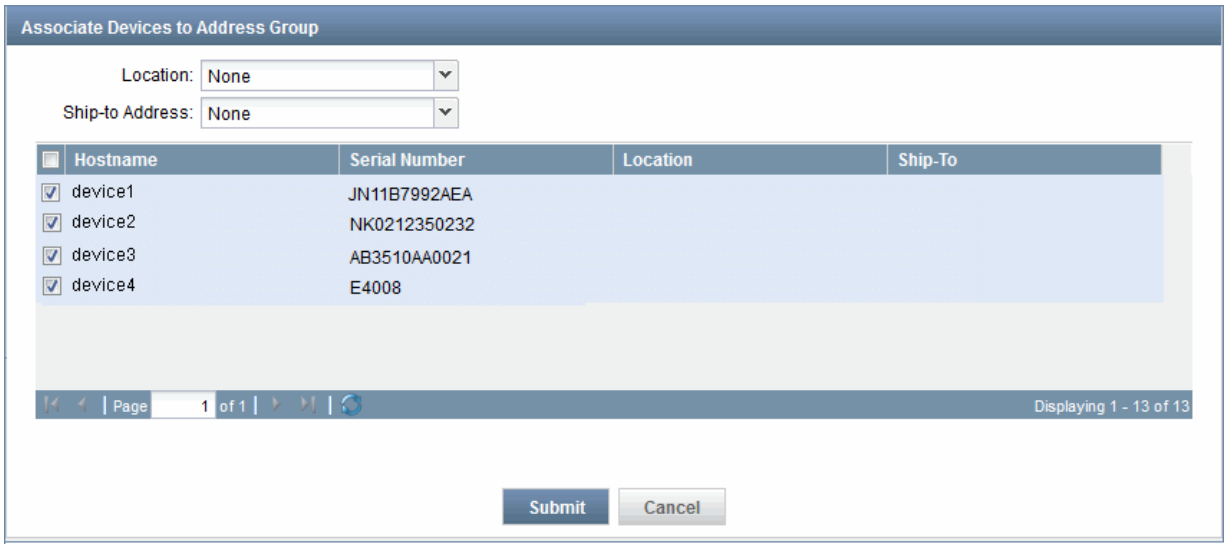
To associate a device to an address group from the Device Groups page:

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

2. Select the device that needs to be associated with an address group, and select **Associate Address Group** from either **Actions** or the right-click menu.

   The Associate Devices to Address Group page appears. This page lists the devices present under this selected device group. The Location and Ship-to Address fields will show address group names if the devices already have an association present in the system. See Figure 91 on page 340.

Figure 91: Associate Devices to Address Group Page



3. Select the devices in the device group to be associated with the address group.

   Selecting the check box to the left of **Hostname** selects all the devices.

4. In the **Location** and **Ship-to Address** fields, select the location and ship-to address of the devices.

5. Click **Submit**.

   All the selected devices will get associated to the new address group and address type.

RELATED DOCUMENTATION

Service Now Device Groups Overview | 137
Associating Devices with an Address Group From the Address Groups Page | 336
Associating Devices with an Address Group From the Organizations Page | 338
Associating Devices with an Address Group from the Service Now Devices Page | 341

Associating Devices with an Address Group from the Service Now Devices Page

Using Service Now, you can associate devices to address groups from the Service Now Devices page.

To associate a device to an address group from Service Now Devices page.

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

2. Select the device needs to be associated with an address group, and select **Associate Address Groups** from either **Actions** or the right-click menu.

   The Associate Devices to Address Group page appears. This page lists the devices present under this selected device group. The Location and Ship-to Address fields will show address group names if the devices already have an association present in the system.

3. In the **Location** and **Ship-to Address** fields, select the location and ship-to address of the devices.

4. Click **Submit**.

   All the selected devices will get associated to the new address group and address type.

RELATED DOCUMENTATION

Service Now Devices Overview | 147
Associating Devices with an Address Group From the Address Groups Page | 336
Associating Devices with an Address Group From the Organizations Page | 338
Associating Devices with an Address Group from the Device Groups Page | 340

16
CHAPTER

Managing E-mail Templates

Service Now E-Mail Templates Overview | 345

Viewing E-Mail Templates | 348

Modifying an E-Mail Template | 350

Service Now E-Mail Templates Overview

You can use Junos Space Service Now to send notifications to users about an event, when it occurs on a device, by e-mails. Service Now provides templates for these e-mails to be sent under various situations such as whan an incident is created, case is created, case and incident are assigned to a user for resolution, or when the incident or case is closed. With administrator privileges, you can modify the content of an e-mail template. However, you cannot delete the default templates.

Service Now displays two types of templates: license-specific and generic e-mail templates based on the mode in which Service Now is operating. For example, if Service Now is operating in Direct mode, the Email Templates page lists templates relevant to Direct mode; If Service Now is working in Partner Proxy mode, the Email templates relevant to Partner Proxy mode are displayed, and so on.

Figure 92: E-Mail Templates Page

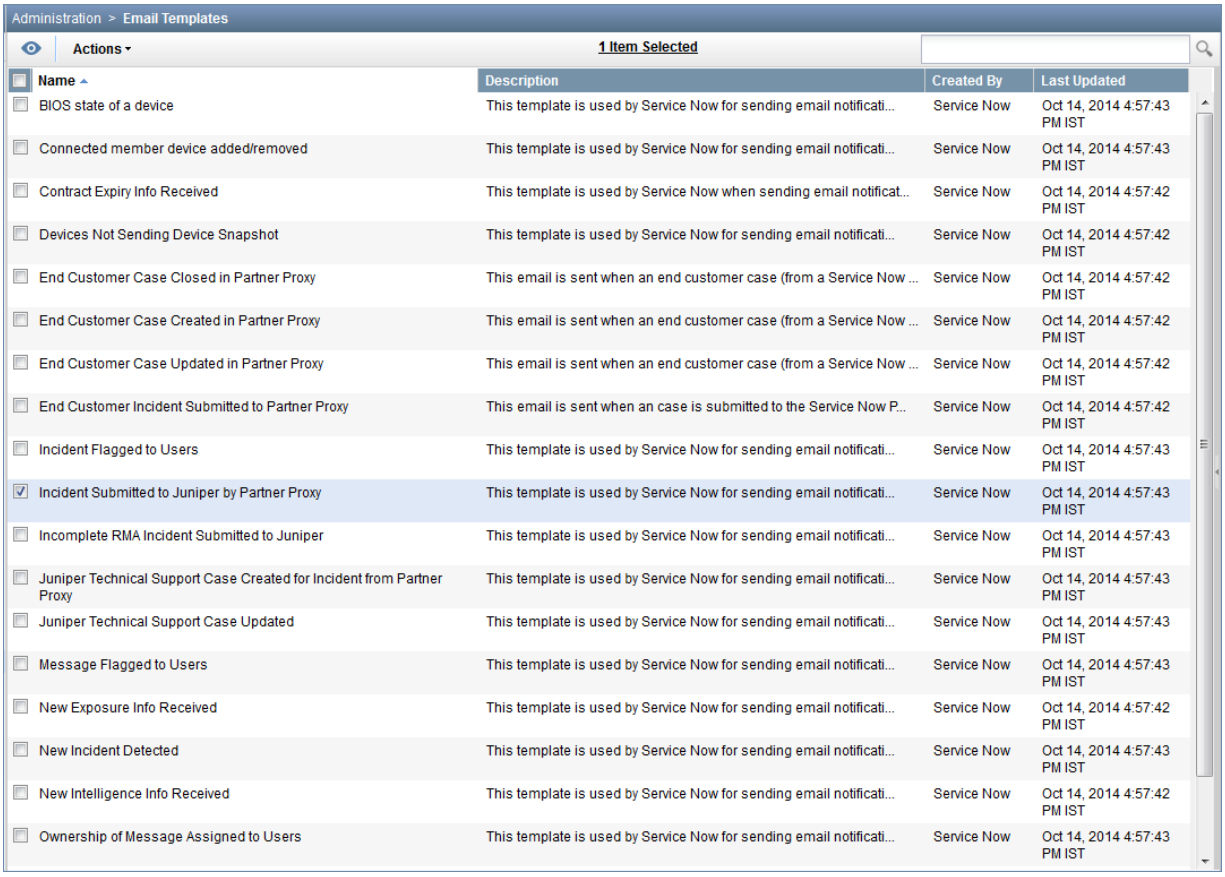


Table 27 on page 346 lists the e-mail templates provided by Service Now and the modes in which the templates can be used.

NOTE: Starting in Service Now Release 16. 1R1, the following e-mail notifications include a five-digit ID of the incident and status of the case created for the incident:

- Incidents flagged to users
- Incidents submitted to JSS
- New incidents detected
- New iJMBs collected from devices

Starting in Service Now Release 17.2R1, the URL in the notification sent out by Service Now includes a fully qualified domain name (FQDN) of the Junos Space server where Service Now is installed instead of the IP address.

The following notifications have FQDN in the URLs:

- Incident Detected
- Incident Submitted
- Case ID Assigned
- Case Status Updated
- End Customer Incident Submitted in Partner Proxy
- End Customer Case Created in Partner Proxy
- End Customer Case Updated in Partner Proxy
- End Customer Case Closed in Partner Proxy

Table 27: List of E-Mail Templates Provided by Service Now and the Modes in which the Templates can be Used

Template Name	Partner Proxy Mode	End Customer Mode	Direct Mode	Offline Mode	Demo Mode
Connected member device added/removed	Yes				
Contract expiry info received	Yes	Yes	Yes		Yes
Devices not Sending Device Snapshot	Yes	Yes	Yes	Yes	Yes
End Customer Case Closed in Partner Proxy	Yes				
End Customer Case Created in Partner Proxy	Yes				

Table 27: List of E-Mail Templates Provided by Service Now and the Modes in which the Templates can be Used *(continued)*

End Customer Case Updated in Partner Proxy	Yes				
End Customer Incident Submitted to Partner Proxy	Yes				
Incident Flagged to Users		Yes			
Incident Submitted to Juniper by Partner Proxy	Yes				
Incident Submitted to Juniper Support Systems			Yes		Yes
Incident Submitted to Connected Junos Space Appliance		Yes			
Incomplete RAM Incident Submitted to Juniper	Yes		Yes		
Incomplete RAM Incident Submitted to Partner Proxy		Yes			
Juniper Technical Support Case Created for Incident from Partner Proxy	Yes				
Juniper Technical Support Case Created for Incident			Yes		Yes
Juniper Technical Support Case Updated	Yes		Yes		Yes
Case Created for Incident		Yes			
Case Updated		Yes			
Message Flagged to Users	Yes	Yes	Yes	Yes	Yes
New Exposure Info Received	Yes	Yes	Yes		Yes
New Incident Detected	Yes	Yes	Yes	Yes	Yes
New Intelligence Info Received	Yes	Yes	Yes		Yes
Ownership of Message Assigned to Users	Yes	Yes	Yes	Yes	
Ownership of Service Now Incident has been Assigned to User	Yes	Yes			Yes

Table 27: List of E-Mail Templates Provided by Service Now and the Modes in which the Templates can be Used *(continued)*

Partner Certificate Expired	Yes	Yes	Yes		Yes
Partner Certificate Expiry	Yes	Yes	Yes		Yes
Product Health Data Collection Failure	Yes	Yes	Yes	Yes	Yes
Switch Over enabled for iJMB	Yes	Yes	Yes	Yes	Yes

Associated Actions

You can perform the following actions related to e-mail templates:

- View e-mail templates; see "Viewing E-Mail Templates" on page 348 for details.
- Modify e-mail templates; see "Modifying an E-Mail Template" on page 350 for details.

Release History Table

Release	Description
16.1R1	Starting in Service Now Release 16. 1R1, the following e-mail notifications include a five-digit ID of the incident and status of the case created for the incident:

RELATED DOCUMENTATION

Service Now Notification Policies Overview

Creating and Editing a Notification Policy

Viewing E-Mail Templates

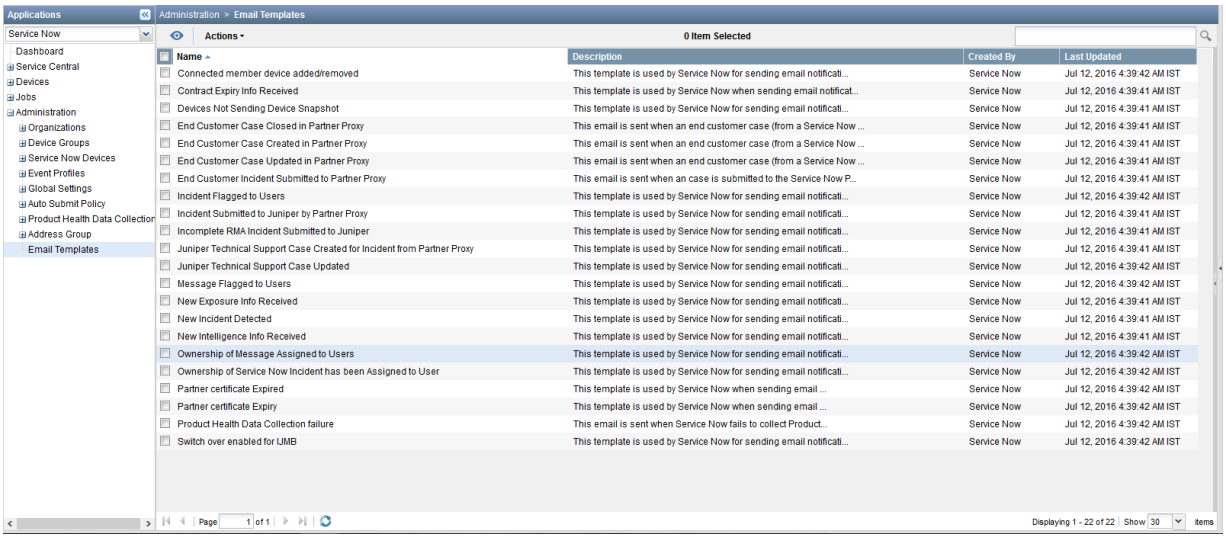
The E-mail templates page in Service Now helps you manage e-mail templates.

To view e-mail templates:

1. From the Service Now navigation tree, select **Administration** > **Email Templates**.

The E-mail Templates page appears as shown in Figure 93 on page 349.

Figure 93: Email Templates Page



2. Double-click the required template from the list.

   The Email Template Details page appears. The Email Template Details page displays the following information about an e-mail template:

   - Name of the template
   - Date and time the template was last updated
   - Description of the template
   - Subject of the e-mail template
   - Information such as JTAC case ID, incident priority, incident ID, and synopsis that you can modify

RELATED DOCUMENTATION

Service Now E-Mail Templates Overview | 345

Modifying an E-Mail Template | 350

Modifying an E-Mail Template

Service Now provides the Modify Email Template option on the Actions list of the Email Templates page to modify the contents of e-mail templates. An e-mail template for an end customer contains $ variables and static content. You cannot modify the $ variables, but you can remove them from the template. All other static content can be modified on a template.

To modify an e-mail template:

1. From the Service Now navigation tree, select **Administration** > **Email Templates**.

   The Email Templates page appears.

2. Select the e-mail template whose content you want to modify and select **Modify** from either the **Actions** list or the right-click menu.

   If a template contains a HTML table, then the Template contents field is followed by table columns in a grid separately. You can remove a column from the template by clearing the check box for that column. The column can be added again by selecting the check box.

RELATED DOCUMENTATION

Service Now E-Mail Templates Overview | 345

Viewing E-Mail Templates | 348

CHAPTER 17

Appendix

Commands Used for Collecting PHD from Managed Devices | 353

Sample Perl Script for Incident and Auto Submit Filters | 357

Commands Used for Collecting PHD from Managed Devices

This topic lists the commands that are executed to collect product health data from routing, switching, and security devices running Junos OS. A command is executed in 1hr, 6hr, or 24 hr intervals on a device.

Commands	Routing Platforms	Switching Platforms	Security Platforms
request pfe execute command "show heap *N*" target *fpc(NUMBER)* where, the values for *N* and *fpc(number)* depend on the platform	6 hr	NA	NA
request pfe execute command "show jnh *N* pool summary" target *fpc(NUMBER)* where, the values for *N* and *fpc(number)* depend on the platform	6 hr	NA	NA
request pfe execute command "show jtree *N* memory extensive" target*fpc(NUMBER)* where, the values for *N* and *fpc(number)* depend on the platform	6 hr	NA	NA
request pfe execute command "show nhdb zones" target *fpc(NUMBER)* where, the values for *N* and *fpc(number)* depend on the platform	6 hr	NA	NA
request pfe execute command "show ukern_tracememory-composition" target *fpc(NUMBER)* where, the values for *N* and *fpc(number)* depend on the platform	6 hr	NA	NA
show arp	NA	6 hr	NA
show chassis alarm | display xml	1 hr	1 hr	1 hr

Commands	Routing Platforms	Switching Platforms	Security Platforms
show chassis cfeb | fpc | scb | SSb The option used with the command depends on the platform.	6 hr	NA	NA
show chassis cluster statistics | display xml	NA	NA	24 hr
show chassis cluster status | display xml	NA	NA	1 hr
show chassis environment	24 hr	24 hr	24 hr
show chassis ethernet-switch	24 hr	24 hr	24 hr
show chassis fabric fpcs	24 hr	24 hr	NA
show chassis fabric plane	NA	NA	24 hr
show chassis fabric plane-location	24 hr	24 hr	NA
show chassis fabric summary	24 hr	24 hr	24 hr
show chassis forwarding	6 hr	NA	NA
show chassis fpc	6 hr	1 hr	NA
show chassis fpc | display xml	1 hr	1 hr	24 hr
show chassis fpc pic-status | display xml	NA	NA	24 hr
show chassis fabricmap	24 hr	24 hr	NA
show chassis hardware | display xml	24 hr	24 hr	NA
show chassis routing-engine | display xml	1 hr	1 hr	1 hr
show ethernet-switching statistics aging	NA	1 hr	NA
show ethernet-switching statistics mac-learning	NA	1 hr	NA
show ethernet-switching table summary	NA	6 hr	NA
show krt queue	1 hr	1 hr	1 hr

Commands	Routing Platforms	Switching Platforms	Security Platforms
show krt state	1 hr	1 hr	1 hr
show pfe statistics error	1 hr	NA	NA
show pfe statistics notification	NA	NA	6 hr
show pfe statistics traffic	1 hr	1 hr	NA
show route summary	6 hr	6 hr	6 hr
show security alg status | display xml	NA	NA	24 hr
show security flow session nat summary | display xml	NA	NA	1 hr
show security flow gate |display xml	NA	NA	6 hr
show security ipsec statistics | display xml	NA	NA	1 hr
show security nat interface-nat-ports | display xml	NA	NA	1 hr
show security idp counters flow	NA	NA	6 hr
show security idp counters packet	NA	NA	6 hr
show security idp security-package-version | display xml	NA	NA	24 hr
show security idp status | display xml	NA	NA	24 hr
show security utm anti-spam statistics | display xml	NA	NA	24 hr
show security utm anti-virus statistics | display xml	NA	NA	24 hr
show security utm anti-virus status | display xml	NA	NA	24 hr
show security utm status | display xml	NA	NA	24 hr

Commands	Routing Platforms	Switching Platforms	Security Platforms
show security utm web-filtering statistics | display xml	NA	NA	24 hr
show security utm web-filtering status | display xml	NA	NA	24 hr
show spanning-tree bridge brief	NA	6 hr	NA
show system buffers | display xml	1 hr	1 hr	6 hr
show system core-dumps | display xml	24 hr	24 hr	24 hr
show system processes extensive	NA	1 hr	1 hr
show system processes extensive no-forwarding	1 hr	NA	NA
show system statistics arp | icmp | icmp6 | ip | ip6 | tcp | tnp The option used with the command depends on the platform.	1 hr	1 hr	NA
show system storage	6 hr	6 hr	6 hr
show system uptime	1 hr	1 hr	1 hr
show system virtual-memory	1 hr	NA	1 hr
show task io	6 hr	6 hr	6 hr
show task memory	6 hr	6 hr	6 hr
show task memory fragmentation	6 hr	NA	NA
show system license | display xml	NA	NA	24 hr
show version | display xml	24 hr	NA	NA
show virtual-chassis protocol adjacency	NA	24 hr	NA
show virtual-chassis protocol statistics	NA	24 hr	NA

Commands	Routing Platforms	Switching Platforms	Security Platforms
show virtual-chassis status	NA	24 hr	NA
show virtual-chassis vc-port	NA	24 hr	NA

RELATED DOCUMENTATION

Service Now Product Health Data Collection Overview

Sample Perl Script for Incident and Auto Submit Filters

The following is a sample Perl script for incident and auto submit filters implemented by using Perl module:

```
#!/usr/bin/perl
use lib qw(/var/cache/jboss/SN/AdvancedFilters /usr/nma/lib
/usr/lib/perl5/vendor_perl/5.8.8);
use MyModule; #Custom_User_Module
use NmaUtil;
use filterUtilV1;

#Input arguments passed from Service Now
$eventType = $ARGV[0];
$deviceHostName = $ARGV[1];
$problemSynopsis = $ARGV[2];
$problemDescription = $ARGV[3];
$osPlatform = $ARGV[4]; # Argument not present in Incident Entity table; present
only as part of JMB
$entity = $ARGV[5];
$junosVersion = $ARGV[6];
$eventTime = $ARGV[7];
$deviceId = $ARGV[8];

#Supported values
[devicePlatform,device_node,customerTrackingNumber,hostName,problemDesc,
problemSynopsis,defectDesc,defectType,prbIdentifier,junosVersion,
occurredTimeStartRange,occurredTimeEndRange]
my %incident_hash = ('hostName'=>'RouterName',
            'occurredTimeStartRange'=> '2018-01-23 10:47:47'
```

```
                                    );

print "MyModule = $MyVariable"; #Using user varibles inside MyModule
print "CheckStatus = ". Verify_CheckStatus(); #Calling user Functions inside MyModule

#getExistingIncidents() will return
[PRBtime,Priority,Severity,defectDesc,defectType,device_node,hostName,prbIdentifier,problemDesc,problemSynopsis,junosVersion]
my $incidents = filterUtilV1::getExistingIncidents(%incident_hash);

print "\n$incidents\n";

if ( $deviceHostName eq 'RouterName' ){
 print "\ntrue";
}
else{
    print "\nfalse";
}
```

NOTE: Do not change the ARG value assigned to a JMB attribute.