



---

# Junos Space

Service Now — Administration

Release

# 1.4



---

Published: 2010-08-16

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

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

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

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

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

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

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

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

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

*Junos Space Service Now User Guide*  
Copyright © 2010, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

Revision History  
August 2010—Junos Space Release 1.4, Revision 1

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

#### YEAR 2000 NOTICE

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

## END USER LICENSE AGREEMENT

**READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).



# Table of Contents

<b>Chapter 1</b>	<b>Administration Overview . . . . .</b>	<b>1</b>
	Administration Overview . . . . .	1
<b>Chapter 2</b>	<b>Organizations . . . . .</b>	<b>5</b>
	Organizations Overview . . . . .	5
	Adding an Organization . . . . .	7
	Adding a Connected Member . . . . .	9
	Modifying Organization Parameters . . . . .	10
	Deleting an Organization . . . . .	11
	Test the Connection to JSS . . . . .	12
	Viewing Messages Assigned to a Connected Member . . . . .	12
	Running an Organization in Test Mode . . . . .	13
<b>Chapter 3</b>	<b>Device Groups . . . . .</b>	<b>15</b>
	Device Groups Overview . . . . .	15
	Creating a Device Group . . . . .	15
	Modifying Device Groups . . . . .	16
	Deleting Device Groups . . . . .	17
<b>Chapter 4</b>	<b>Devices . . . . .</b>	<b>19</b>
	Service Now Devices Overview . . . . .	19
	Adding Devices from the Platform . . . . .	21
	Installing AI-Scripts on Devices Using Service Now . . . . .	22
	Installing AI-Scripts Manually on Devices . . . . .	23
	Uninstalling AI-Scripts from Devices . . . . .	25
	Exporting Device Data in CSV and Excel Format . . . . .	25
	Deleting a Device . . . . .	26
	Associating Devices to a Device Group . . . . .	26
<b>Chapter 5</b>	<b>Script Bundles . . . . .</b>	<b>27</b>
	AI-Scripts Overview . . . . .	27
	What AI-Scripts Do . . . . .	27
	Events Detected by AI-Scripts . . . . .	27
	JMB Contents . . . . .	28
	Adding a Script Bundle to Service Now . . . . .	28
	Deleting a Script Bundle from Service Now . . . . .	29
<b>Chapter 6</b>	<b>Global Settings . . . . .</b>	<b>31</b>
	Configuring Global Settings . . . . .	31
	Adding an SNMP Server . . . . .	34
	Editing and Deleting an SNMP Server . . . . .	35
	Configuring Proxy Server Settings . . . . .	36

<b>Chapter 7</b>	<b>Service Now Contract and User Roles . . . . .</b>	<b>37</b>
	Service Contract . . . . .	37
	Service Now User Roles . . . . .	38
<b>Chapter 8</b>	<b>Index . . . . .</b>	<b>41</b>
	Index . . . . .	43



## CHAPTER 1

# Administration Overview

- Administration Overview on page 1

## Administration Overview

---

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

Devices with AI-Scripts installed periodically send device data in the form of Informational Juniper Message Bundles (iJMBs) to Service Now . Users can view this information. Using Service Now you can add and manage devices, upload AI-Script bundles, and install the AI-Scripts on the devices. You can add devices that are part of the Junos Space platform to Service Now and group them under organizations.

An organization is defined by a unique site id that is a unique identifier of a customer record in Juniper Networks CRM systems. After creating an organization, you can test its connectivity with JSS and even run it in test mode. JSS provides support for the incidents and iJMBs that you submit depending on your service contract level. J-Care Efficiency, Continuity, or Agility levels of service are required to use Service Now.

If you are a Juniper Networks partner or a direct customer with multiple distinct networks, you can use multiple Service Now organizations to keep customers or networks separate. Service Now organizations are defined by the site ID (used when opening support cases) under devices and users. Also, by associating an organization with one or more device groups, you can maintain groups of devices with similar attributes and control a user's access to devices. Device groups also help you automatically install AI-Scripts on many devices at one time.

Some administration tasks, such as adding connected members and viewing messages assigned to them, are enabled only when Service Now partner proxy mode is activated. For more information on Service Now modes, see Service Now Modes .

The Service Now sidebar includes a Getting Started section that guides the administrator through the initial setup required to get the application up and running. This section lists four required and two optional tasks. Clicking the task links displays the respective pages in the Inventory panel where these tasks can be performed.

The required tasks are:

1. Reviewing global settings.
2. Creating an organization.
3. Adding devices to Junos Space.
4. Creating a device group.
5. Installing AI-Scripts on devices.

The optional task is adding a new script bundle.

The Administration page graphically displays information about devices with respect to the device group they belong to, whether these devices are sending device snapshots periodically, and also the devices that have never sent device snapshots to Service Now. Using the Administration tab, you can perform the following tasks:

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

For more information, see the Junos Space documentation on the Juniper Networks technical documentation page.

**Related Topics**

- Service Now Modes
- Service Now Devices Overview on page 19
- Device Groups Overview on page 15
- AI-Scripts Overview on page 27
- Organizations Overview on page 5

- [Configuring Global Settings on page 31](#)
- [Service Contract on page 37](#)



## CHAPTER 2

# Organizations

- Organizations Overview on page 5
- Adding an Organization on page 7
- Adding a Connected Member on page 9
- Modifying Organization Parameters on page 10
- Deleting an Organization on page 11
- Test the Connection to JSS on page 12
- Viewing Messages Assigned to a Connected Member on page 12
- Running an Organization in Test Mode on page 13

## Organizations Overview

---

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

Device groups are used to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. Using device groups, you can control the access that users have over devices. See “Device Groups Overview” on page 15.

For more information about creating device groups, see “Creating a Device Group” on page 15.

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

Service Now organizations are displayed on the **Manage Organizations** page. You can choose to display the organizations either as a table arranged according to name, site ID, submit cases as, username, and connection status, or as icons, as shown in Figure 1 on page 6.

Figure 1: Manage Organizations Page



Table 1 on page 6 describes the fields displayed in the tabular view of the **Manage Organizations** page and in the **Organizations Details** dialog box.

Table 1: Organization Column Descriptions

Column Name	Description
Name	Name of the organization
Site ID	Identifier for the Customer Site in the JTAC Clarify system.
Submit Cases As	Status of the case that is sent to JSS. It is a real case or a test case that is sent in a production environment. The synopsis of a test case sent to JSS is appended with [Test Mode].
User Name	Name used to identify the user for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases.
Connection Status	Status of the connection between the organizations and JSS.
JMB Filter Level	Amount of device configuration information in a JMB that can be shared with JSS

From the Organizations page, you can:

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

**Related Topics** • Adding an Organization on page 7

- Modifying Organization Parameters on page 10
- Running an Organization in Test Mode on page 13

## Adding an Organization

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



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

To add a Service Now organization:

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

The **Add Organization** dialog box is displayed.

The screenshot shows the 'Add Organization' dialog box. It has a title bar 'Add Organization'. Inside, there are several input fields: 'Name' (with a red exclamation mark icon), 'Site ID' (with a red exclamation mark icon), 'Submit Cases as:' (a dropdown menu showing 'Real Cases'), 'User Name:', 'User Password:', 'Confirm User Password:', and 'JMB Filter Level:' (a dropdown menu showing 'Do not send'). At the bottom, there are two buttons: 'Submit' (blue) and 'Cancel' (red).

2. Enter the organization parameters in the provided fields.  
For a detailed description of these fields, see Table 2 on page 8.
3. Click **Submit**.

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

Table 2 on page 8 defines the **Add Organization** dialog box fields.

Table 2: Organization Credentials Page Field Descriptions

Name	Description	Privileges	Range/Length	Default
Name	Name of the organization	Service Now Admin Privileges	64 characters	Blank
Site ID	Identifier for the Customer Site in the JTAC Clarify system.	Service Now Admin Privileges	80 characters	Blank
Submit cases as	Status of the case that is sent to JSS. It is a real case or a test case that is sent in a production environment. The synopsis of a test case sent to JSS is appended with [Test Mode].	Service Now Admin Privileges	<ul style="list-style-type: none"> <li>Real Cases</li> <li>Test Cases</li> </ul>	Disabled
User Name	Name used to identify the user for communications with the JTAC Clarify system, such as creating cases, and checking for updates to existing cases.	Service Now Admin Privileges	32 characters	Blank
User Password	Password used to login, for the account with the user name you specify.	Service Now Admin Privileges	32 characters	Blank
Confirm User Password	Password for confirmation must match the value in User Password field.	Service Now Admin Privileges	32 characters	Blank
JMB Filter Level	Amount of device configuration information in JMBs to be shared with JSS: <ul style="list-style-type: none"> <li>Do not send—Sends no configuration information.</li> <li>Send all information except configuration—Sends all device information except the configuration.</li> <li>Send all information with IP Addresses overwritten—Sends all device information, except IP addresses</li> <li>Send all information—Sends all device information.</li> <li>Only send list of features used—Sends only the device configuration information.</li> </ul>	Service Now Admin privileges	Not applicable.	Do not send

- Related Topics**
- Organizations Overview on page 5
  - Running an Organization in Test Mode on page 13



## Adding a Connected Member

After you configure Service Now to run in partner proxy mode, you can add multiple end customers and manage end customer Service Now applications over a secure https connection. The partner proxy can communicate with the end customer only after the Service Now application of an end customer is activated. For more information about partner proxy and end customer modes, see *Service Now Modes*.



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

To add a connected member to Service Now:

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

The **Add Member** dialog box is displayed as shown in Figure 2 on page 9.

**Figure 2: Add Member Dialog Box**

2. Enter a name for the connected member.  
The name must begin with an alphanumeric character (a-z, 0-9), and can contain underscores (\_), spaces, and hyphens (-).
3. Enter a username for the connected member.  
The username must be in the format user@example.com.
4. Enter the password that can be used to log in with the user name you have entered.
5. Enter the same password again to confirm.
6. Select one of the following values to specify the amount of device configuration information in a JMB that can be shared with JSS:
  - Do not send—Sends no configuration information.
  - Send all information except configuration—Sends all device information except the configuration.

- Send all information with IP Addresses overwritten—Sends all device information, except IP addresses
  - Send all information—Sends all device information.
  - Only send list of features used—Sends only the device configuration information.
7. Select the organization with which the end customer can be associated. Ensure that you select an organization that has partner proxy credentials.
  8. Click **Submit**.

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

- Related Topics**
- Adding an Organization on page 7
  - Organizations Overview on page 5

---

## Modifying Organization Parameters

---

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



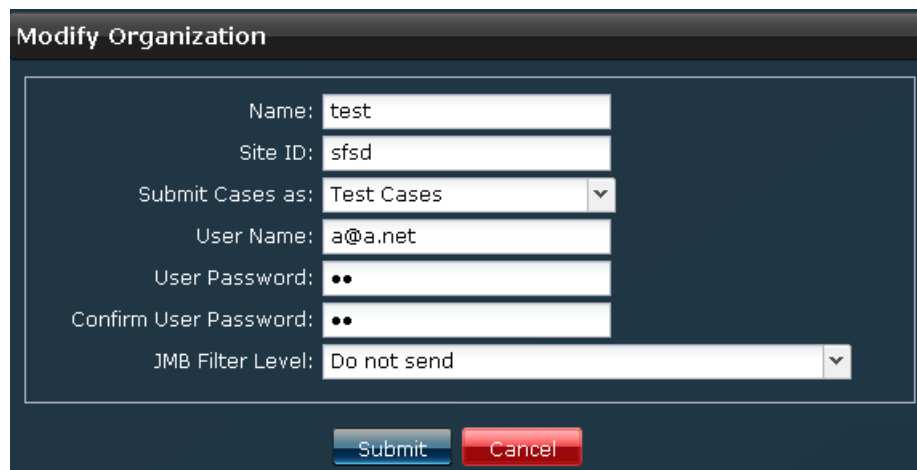
**NOTE:** When you modify the parameters of a connected member, you cannot edit the name of the connected member and the organization associated with it. For more information about connected members see [Service Now Modes](#).

To modify the parameters of an organization:

1. From the Service Now task ribbon, select **Administration > Organizations**.  
The **Manage Organizations** page is displayed.
2. Select the organization whose parameters you want to modify.
3. Click **Modify Organization** from the Actions panel.

The **Organizations** dialog box displays the name, site ID, submit cases as, user name, and password, and the JMB filter level of the selected organization.

Figure 3: Modify Organization Dialog Box



4. Make your changes to these parameters.
5. Click **Submit**.

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

- Related Topics**
- Organizations Overview on page 5
  - Running an Organization in Test Mode on page 13

## Deleting an Organization

You can use the Service Now **Manage Organizations** page to delete organizations. To do this, you need Service Now Admin privileges.

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

To delete an organization:

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

The **Manage Organizations** page is displayed.

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

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

4. Click **Delete**.

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



**NOTE:** Deleting an organization also removes associated device groups.

- Related Topics**
- Organizations Overview on page 5
  - Running an Organization in Test Mode on page 13

---

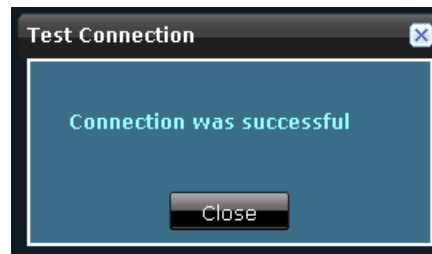
## Test the Connection to JSS

From the **Manage Organizations** page, you can test an organization's connectivity with Juniper Support Systems (JSS). This test can be performed with every organization in the table.

To test an organization's connectivity with JSS:

1. From the Service Now task ribbon, select **Administration > Organizations**.  
The **Manage Organizations** page is displayed.
2. Select the organization whose connection to JSS you want to test.
3. Click **Check Status** from the Actions panel.

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



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

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

- Related Topics**
- Organizations Overview on page 5
  - Running an Organization in Test Mode on page 13

---

## Viewing Messages Assigned to a Connected Member

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

To view the messages assigned to a connected member:

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

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

2. Select the connected member whose list of assigned messages you want to view.
3. Right-click your selection or use the **Actions** panel and select **View Messages**.

As shown in Figure 4 on page 13, the **Messages assigned to Connected Member** page displays the list of messages assigned to the selected connected member.

**Figure 4: Messages Assigned to Connected Member page**

Messages assigned to Connected Member		
<a href="#">Return to Organization</a>		
Title ▲	Status	Sent
<a href="#">abc</a>	Delivered	2010/05/07 01:36
<a href="#">final1</a>	Delivered	2010/05/07 01:36

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

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

5. Click **Return to Organization** to return to the **Manage Organizations** page.

- Related Topics**
- Assigning a Message to a Connected Member
  - Messages Overview

## Running an Organization in Test Mode

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

To run an organization in test mode:

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

The **Manage Organizations** page is displayed. If the table is empty, you need to add organizations.

2. Select the organizations that you want to place in test mode.
3. Select **Modify Organization** from the Actions list.

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

4. Set the **Submit Cases as** drop-down menu value to **Test Cases**.
5. Click **Submit**.

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

**Related Topics**

- Organizations Overview on page 5
- Modifying Organization Parameters on page 10

## CHAPTER 3

# Device Groups

- Device Groups Overview on page 15
- Creating a Device Group on page 15
- Modifying Device Groups on page 16
- Deleting Device Groups on page 17

### Device Groups Overview

---

You use device groups to group devices within an organization. By associating an organization with one or more device groups, you can maintain groups of devices with similar attributes or uses. You can associate one or more devices with every device group

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

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

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

- Related Topics**
- Creating a Device Group on page 15
  - Modifying Device Groups on page 16
  - Deleting Device Groups on page 17

### Creating a Device Group

---

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

To create a device group:

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

The **Administration: Create Device Group** page is displayed.

Administration: Create Device Group

Name:

Organizations:  [New Organization](#)

Select Devices to add them to the Device Group

<input type="checkbox"/>	Host Name	Platform	Network Name	Serial Number	Version
--------------------------	-----------	----------	--------------	---------------	---------

Page 1 of 1 | No results to display

[Add](#) [Cancel](#)

2. Enter a name for the device group within the **Name** field.  
The name must begin with a letter and can have only alphanumeric characters (a-z, 0-9), underscores(\_), and hyphens (-).
3. In the **Organizations** drop-down list, select an organization for this device group.  
If you want to add a new organization, click **New Organization**. See “Adding an Organization” on page 7.
4. Select the devices that you want to add to this device group.
5. Click **Finish**.

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

- Related Topics**
- Device Groups Overview on page 15
  - Modifying Device Groups on page 16

## Modifying Device Groups

You can modify the parameters of a device group in Service Now.

To modify a device group:

1. From the Service Now task ribbon, select **Administration > Device Groups**.  
The **Manage Device Group** page lists the existing device groups.
2. Select the device group whose parameters you want to modify.



3. Click **Modify Device Group** from the Actions panel.

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

4. Make your modifications.  
Use the **Device Groups** navigation panel on the right to add or delete devices from the selected device group.

5. Click **Finish**.

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

- Related Topics**
- Device Groups Overview on page 15
  - Deleting Device Groups on page 17
  - Creating a Device Group on page 15

## Deleting Device Groups

---

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

To delete a device group:

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

The **Manage Device Group** page lists the existing device groups.

2. Select the device group that you want to delete.
3. Click **Delete Device Group** from the Actions panel.

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

4. Click **Delete**.

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

- Related Topics**
- Device Groups Overview on page 15
  - Modifying Device Groups on page 16



## CHAPTER 4

# Devices

- Service Now Devices Overview on page 19
- Adding Devices from the Platform on page 21
- Installing AI-Scripts on Devices Using Service Now on page 22
- Installing AI-Scripts Manually on Devices on page 23
- Uninstalling AI-Scripts from Devices on page 25
- Exporting Device Data in CSV and Excel Format on page 25
- Deleting a Device on page 26
- Associating Devices to a Device Group on page 26

### Service Now Devices Overview

---

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

After you add devices and create device groups, you can perform various operations on them, such as installing and uninstalling AI-Scripts individually on every device or on all the devices in a device group at once, and also deleting them from the Service Now database. Service Now devices are displayed on the **Service Now Devices** page. You can choose to display the devices either as a table arranged according to organization, device group, hostname, serial number, platform, version, and script bundle, or as icons, as shown in Figure 5 on page 20. Table 3 on page 20 describes the columns in the **Service Now Devices** page and the **Device Detail** dialog box.

Figure 5: Service Now Devices Page



Table 3 on page 20 describes the fields displayed in the tabular view of the **Service Now Devices** page and in the **Device Details** dialog box.

Table 3: Service Now Devices Column Descriptions

Field Name	Description
HostName	Unique name by which the device is known on a network.
Serial Number	Serial number of device.
Platform	Type of device (routing platform).
OS Version	Version of the Junos operating system that is running on the device.
Organization	Name of the organization to which this device belongs.
Device Group	Name of the device group to which this device belongs.
Script Bundle	Name and version of the script bundle installed on the device.
Connection Status	Status of connection from the device to Service Now.
Device Snapshot Status	Status of iJMB upload.
Service SKU	Code that identifies the name of the Service Now contract purchased.

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

- Add devices from the platform
- Install AI-Script on devices

- Uninstall AI-Script from devices
- Export device data into CSV and Excel format
- Modify device parameters
- Delete devices
- Associate devices with a device group

#### Related Topics

- Adding Devices from the Platform on page 21
- Installing AI-Scripts on Devices Using Service Now on page 22
- Uninstalling AI-Scripts from Devices on page 25
- Exporting Device Data in CSV and Excel Format
- Modifying Device Groups on page 16
- Deleting a Device on page 26
- Associating Devices to a Device Group on page 26

## Adding Devices from the Platform

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



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

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

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

The **Select Devices to Add to Service Now and Click Next or Finish** page displays the devices that have not been added to Service Now.

Select Devices to Add to Service Now and Click Next or Finish					Add Devices	
<input type="checkbox"/>	Host Name	Network Name	SSH User Name	SSH Password	Device Status	
<input type="checkbox"/>	puppy	10.204.92.75	regress	*****	Imported	<a href="#">Add Devices</a>
<input type="checkbox"/>	junoscopea	10.204.92.63	regress	*****	Imported	<a href="#">Install AI Scripts</a>

2. Select the devices that you want to add.
3. (Optional) To install script bundles on the selected devices, click **Install AI Scripts** or click **Next**, and check the **Install AI Scripts on new Devices** check box.

For more information about installing AI-Scripts on devices, see “Installing AI-Scripts on Devices Using Service Now” on page 22. If you are unable to install AI-Scripts, ensure that the device has proper login credentials and belongs to a device group.

4. Click **Finish**.

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

**Related Topics** • Service Now Devices Overview on page 19

## Installing AI-Scripts on Devices Using Service Now

AI-Scripts installed on Juniper Networks devices provide the information needed to automatically detect and report problem (incident) and information events, thus ensuring maximum network uptime. Service Now uses Device Management Interface (DMI) to install and uninstall AI-Scripts on devices. DMI is an extension to the NETCONF network management protocol.



**NOTE:** While operating in Partner Proxy mode, you cannot install AI-Scripts on a connected member's device.

To install AI-Scripts on devices:

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

The **Service Now Devices** page is displayed.

2. Select the device on which you want to install the script bundle.



**NOTE:** You can install AI-Scripts only on devices that have proper login credentials and belong to a device group.

3. Click **Install AI-Scripts** from the Actions panel.

The **Install AI-Script** dialog box is displayed.

4. Select a script bundle from the **AI-Script Bundle Name** drop-down list, which displays the script bundles that Service Now manages.

If you want to add a new script bundle, click **Add Script Bundle**. For more information about how to add a script bundle, see “Adding a Script Bundle to Service Now” on page 28.

5. If you do not want to save a copy of the script bundle file during installation on the device, select the **Never store Script Bundle files on the device** check box.
6. If you want to remove the script bundle from the device, after the installation, select the **Remove Script Bundle files after successful installation** check box.
7. If you want to schedule a time for installation, select the **Schedule a Later Time** check box, and specify the **Start Date and Time** for the installation. The installation process begins automatically at the time you specify.
8. Click **Submit**.

The AI-Script installation task is scheduled and the Job Information window displays the job ID.



If you want to verify the status of the AI-Script installation task on the selected devices, click the job ID link. The **Manage Jobs** page displays the status of the job.

- Related Topics**
- AI-Scripts Overview on page 27
  - Installing AI-Scripts Manually on Devices on page 23
  - Adding a Script Bundle to Service Now on page 28

## Installing AI-Scripts Manually on Devices

AI-Scripts can be installed on Junos OS devices manually using CLI mode. Service Now also uses the loopback interface on Junos OS devices for collecting the Juniper Message Bundle (JMB) when an event occurs.



**NOTE:** If you do not want to use loopback address, you can use the management IP address for collecting JMBs in the archive-sites [/var/tmp].

To enable communication using the loopback address, add the following firewall rules:

```
set firewall family inet filter scp-block term ais-scp from source-address
127.0.0.1/32
```

```
set firewall family inet filter scp-block term ais-scp from destination-address
127.0.0.1/32
set firewall family inet filter scp-block term ais-scp from protocol tcp
set firewall family inet filter scp-block term ais-scp from port 22
set firewall family inet filter scp-block term ais-scp then accept
Rouer001# show firewall family inet filter scp-block term ais-scp
from { source-address {
127.0.0.1/32;
}
destination-address {
127.0.0.1/32;
} protocol tcp;
port 22;
}
then accept;
```



**NOTE:** For manual installation of AI-Scripts on a device, you require the login credentials used to discover devices in Junos Space.

To install AI-Scripts manually:

1. Copy the AI-Script bundle (example: jais-2.1R2.0-signed.tgz) to the Junos OS device using SCP or FTP.
2. From configuration mode, execute the following commands:  
**set groups juniper-ais system scripts commit allow-transients**  
**set groups juniper-ais system scripts commit file jais-activate-scripts.slax optional**  
**set groups juniper-ais interfaces lo0 unit 0 family inet address 127.0.0.1/32**  
**set groups juniper-ais event-options destinations juniper-aim archive-sites**  
**"scp://<user>@127.0.0.1://var/tmp" password <password for user>**
3. Install the AI-Script bundle in the CLI mode using the command  
**request system scripts add <full-path>/jais-2.1R2.0-signed.tgz**

The AI-Script is installed on the device.

- Related Topics**
- Installing AI-Scripts on Devices Using Service Now on page 22
  - Adding a Script Bundle to Service Now on page 28



---

## Uninstalling AI-Scripts from Devices

---

You can use Service Now to uninstall AI-Scripts from devices. You cannot uninstall these scripts from devices that do not have proper login credentials. Service Now uses Device Management Interface (DMI) to install and uninstall AI-Scripts on devices. DMI is an extension to the NETCONF network management protocol.



**NOTE:** While operating in Partner Proxy mode, you cannot uninstall AI-Scripts from a connected member's device.

To uninstall an AI-Script from devices:

1. From the Service Now task ribbon, select **Administration > Service Now Devices**.  
The **Service Now Devices** page is displayed.
2. Select the device from which you want to uninstall the script bundle.
3. Click **Uninstall AI-Scripts** from the Actions panel.  
You are prompted to confirm the deletion.
4. Click **Submit**.  
This AI-Script is removed from the selected device.

- Related Topics**
- AI-Scripts Overview on page 27
  - Installing AI-Scripts on Devices Using Service Now on page 22

---

## Exporting Device Data in CSV and Excel Format

---

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

To export the device data in CSV and Excel format:

1. From the Service Now task ribbon, select **Administration > Service Now Devices**.  
The **Service Now Devices** page is displayed.
2. Select the device whose data you want to export.
3. Click **Export Devices** from the Actions panel.  
The **Export Devices** dialog box displays the links to the CSV and Excel files.
4. Select the links to save the files in CSV and Excel file formats.

- Related Topics**
- Service Now Devices Overview on page 19
  - Deleting a Device on page 26

## Deleting a Device

---

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

To delete a device from Service Now:

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

The **Service Now Devices** page lists the Service Now devices.

2. Select the device that you want to delete.

3. Click **Delete** from the Actions panel.

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

4. Click **Delete** again.

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

- Related Topics**
- Service Now Devices Overview on page 19
  - Modifying Device Groups on page 16

## Associating Devices to a Device Group

---

Service Now associate devices with device groups.

To associate devices with device group:

1. From the Service Now task ribbon, 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.

3. Click **Associate Device Groups** from the Actions panel.

The **Associate Device Groups** dialog box is displayed.

4. In the Device Group drop-down list, select the device group that you want to associate with the selected device.

5. Click **Submit**.

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

- Related Topics**
- Service Now Devices Overview on page 19
  - Modifying Device Groups on page 16

## CHAPTER 5

# Script Bundles

- AI-Scripts Overview on page 27
- Adding a Script Bundle to Service Now on page 28
- Deleting a Script Bundle from Service Now on page 29

### AI-Scripts Overview

---

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

- What AI-Scripts Do on page 27
- Events Detected by AI-Scripts on page 27
- JMB Contents on page 28

### What AI-Scripts Do

AI-Scripts perform the following functions:

- React to specific incident events that occur on devices and provide relevant information about the problems for analysis
- Periodically collect data on events that can be used to predict and prevent risks in the future.
- Package all incident and information event data into a structured format called a Juniper Message Bundle (JMB) and send it to Service Now. You can configure Service Now to send event data to Juniper Support Systems (JSS). JSS collects incident and device snapshots from Service Now and sends information messages back to Service Now specifically for your network.

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

### 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

## JMB Contents

The JMB for incidents and informational JMBs contains the following:

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

- Related Topics**
- Adding a Script Bundle to Service Now on page 28
  - Deleting a Script Bundle from Service Now on page 29

---

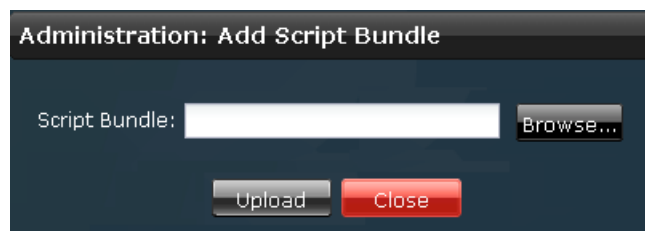
## Adding a Script Bundle to Service Now

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

To add a script bundle:

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

The **Administration: Add Script Bundle** page is displayed.



The screenshot shows a web interface titled "Administration: Add Script Bundle". It has a dark blue header. Below the header, there is a label "Script Bundle:" followed by a white text input field. To the right of the input field is a "Browse..." button. At the bottom of the form, there are two buttons: "Upload" and "Close".

2. Click **Browse**.

The File Upload window is displayed.

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

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

- Related Topics**
- AI-Scripts Overview on page 27
  - Deleting a Script Bundle from Service Now on page 29

---

## Deleting a Script Bundle from Service Now

---

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



NOTE: You cannot delete the preloaded script bundle that is available in the application.

To delete a script bundle:

1. From the Service Now task ribbon, select **Administration > Script Bundles**.

The **Manage Script Bundles** page lists the available script bundles.

2. Select the script bundle that you want to delete.
3. Click **Delete Script Bundles** from the Actions panel.

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

4. Click **Delete**.

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

- Related Topics**
- [AI-Scripts Overview on page 27](#)
  - [Adding a Script Bundle to Service Now on page 28](#)



## CHAPTER 6

# Global Settings

- Configuring Global Settings on page 31
- Adding an SNMP Server on page 34
- Editing and Deleting an SNMP Server on page 35
- Configuring Proxy Server Settings on page 36

### Configuring Global Settings

---

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

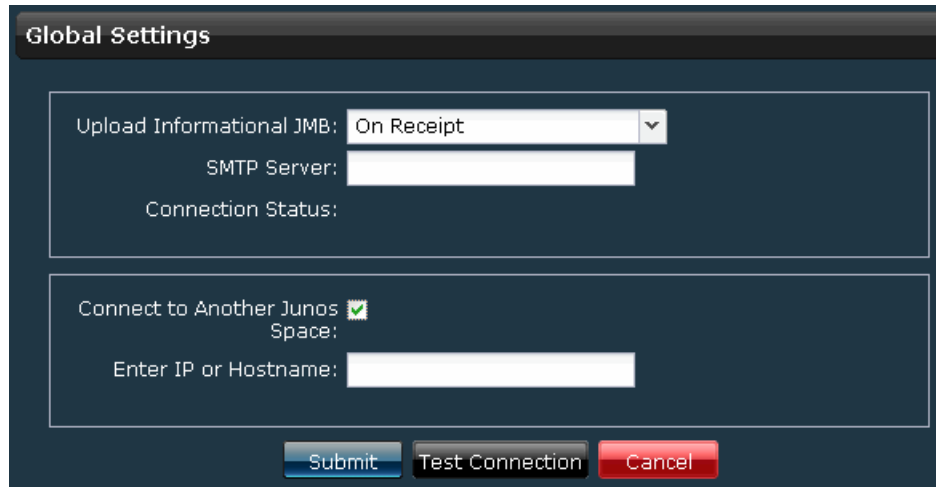
- Set the interval to scan devices for informational JMBs.
- Set the SMTP server (IP address / hostname).
- Verify Service Now to JSS or Service Now to partner proxy (from end customer mode) connection status.
- Connect the end customer's Service Now application to the partner proxy.

Using the Service Now **Global Settings** page, a Service Now end customer can also connect to a partner's Service Now application. When an end customer connects to a partner, Junos Space uses a self-signed security certificate. Although this method of identification is not trusted, Junos Space automatically accepts this certificate to ensure that the communication between the partner and the end customer is encrypted. After you connect to the partner proxy's Service Now application, you enter end customer mode and you cannot revert back to standard, or partner proxy modes. After you connect to the partner you can add an organization using the credentials provided by the partner. See "Adding an Organization" on page 7. After the connection of the organization is validated, you can submit incidents and iJMBs to, and open cases with, the Service Now partner.

For more information about standard, partner, and end customer modes, see Service Now Modes .

To configure Service Now Global settings:

1. From the Service Now task ribbon, select **Administration > Global Settings**.  
The **Global Setting** page is displayed.



2. Add your Service Now settings.  
For a description of the **Global Setting** page fields see Table 5 on page 33.



**NOTE:** The **Connect to Another Junos Space** check box is available only in Service Now end customer mode.

3. Click **Test Connection**.  
The connection to JSS is tested and the result is displayed as **JSS Connection Status**.
4. Click **Submit**.  
This action saves the Service Now settings that you specified and updates the Service Now service with these new settings.

Table 4 on page 32 describes the **Global Setting** page command buttons.

**Table 4: Global Settings Command Button**

Button Name	Description	Privileges	Enabled/Disabled	Results
Submit	Saves any modified Service Now global settings and updates the Service Now service with these new settings.	Service Now Admin Settings	Enabled if you have admin privileges	Saves settings that were modified.
Test Connection	<ul style="list-style-type: none"> <li>In standard, or partner proxy mode, verifies the organization connectivity with JSS.</li> <li>In the end-customer mode, verifies the organization connectivity with the partner's Service Now application.</li> </ul>	Service Now Admin Settings	Enabled if you have admin privileges	Displays the Connection Status as Success or Failed.



Table 4: Global Settings Command Button (*continued*)

Button Name	Description	Privileges	Enabled/Disabled	Results
Cancel	Withdraws the submission of modified settings.	Service Now Admin Settings	Not applicable.	Navigates back to the <b>Global Settings</b> page without saving the entries.

Table 5 on page 33 describes the fields displayed in the tabular view of the **Global Settings** page.

Table 5: Global Settings Parameters

Name	Description	Privileges	Range/Length	Default
Upload Informational JMB	Interval when a newly detected Informational JMB is sent to JSS: <ul style="list-style-type: none"> <li>On Receipt</li> <li>Daily</li> <li>Weekly</li> </ul>	Service Now Admin privileges	Not applicable.	On Receipt
SMTP Server	Destination server that Service Now can use to send information. <ul style="list-style-type: none"> <li>IP Address: IP address of network management station where Service Now trap destination are sent.</li> <li>Hostname: Identifier used for network communication between Service Now and JUNOS device. For example, it can be a hostname (host-name.juniper.net) or an IP address.</li> </ul>	Service Now Admin privileges	255 characters	Blank
Connection Status	Status of connection from Service Now to JSS.  If Service Now is operating in end customer mode, the connection status between Service Now and the partner proxy is displayed.	Service Now Partner	<ul style="list-style-type: none"> <li>Success — URL is responsive</li> <li>No route to host</li> <li>Connection refused</li> <li>The Home Base server is temporarily unable to service your request</li> </ul>	Blank
Connect to Another Junos Space	IP address or hostname of the Service Now partner proxy that can be used to send and receive information from the partner proxy.  This field is not displayed when Service Now operates in standard mode and partner proxy mode.	Service Now End Customer	Not Applicable	Blank

**Related Topics** • Organizations Overview on page 5

- Configuring Proxy Server Settings on page 36

## Adding an SNMP Server

---

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

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

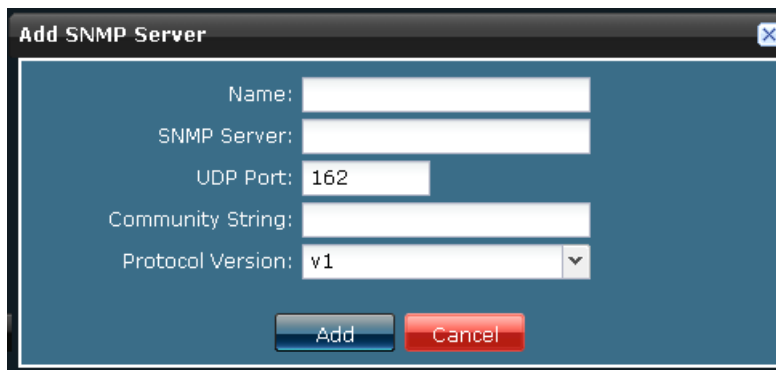
To add an SNMP server:

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

The **SNMP Servers** page is displayed.

2. Click **Add**.

The **Add SNMP Server** dialog box is displayed.

The image shows a dialog box titled "Add SNMP Server" with a close button in the top right corner. The dialog has a dark blue header and a lighter blue body. It contains five input fields: "Name:" (text box), "SNMP Server:" (text box), "UDP Port:" (text box with "162" entered), "Community String:" (text box), and "Protocol Version:" (dropdown menu with "v1" selected). At the bottom, there are two buttons: "Add" (blue) and "Cancel" (red).

3. Enter a name for the SNMP server, using alphanumeric values.
4. Enter the SNMP server that is the IP address or hostname of network management station where Service Now SNMP traps are sent.  
Do not use special characters.
5. Enter the UDP port.  
The User Data Protocol (UDP) port is a mechanism whereby a computer can simultaneously support multiple communication sessions with other computers and programs on the network. A port directs the request to a particular service that can be found at that IP address. The default UDP Port number is 162.
6. Enter a community string using only alphanumeric characters.  
A community string is a password that allows access to a network device. It defines the community of people that can access the SNMP information on the device.
7. Select the protocol version from the drop-down list box that specifies the SNMP versions.
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 receiver such as HP OpenView to monitor the devices with SNMP, the following MIB files must be loaded. The file **jnx-smi.mib** must be loaded first:

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

- Related Topics**
- Configuring Global Settings on page 31
  - Configuring Proxy Server Settings on page 36

---

## Editing and Deleting an SNMP Server

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

### Editing an SNMP Server

To edit an SNMP server:

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

The **SNMP Servers** page is displayed.

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

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

### Deleting an SNMP Server

To delete an SNMP server:

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

The **SNMP Servers** page is displayed.

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

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

- Related Topics**
- Configuring Global Settings on page 31
  - Configuring Proxy Server Settings on page 36

## Configuring Proxy Server Settings

---

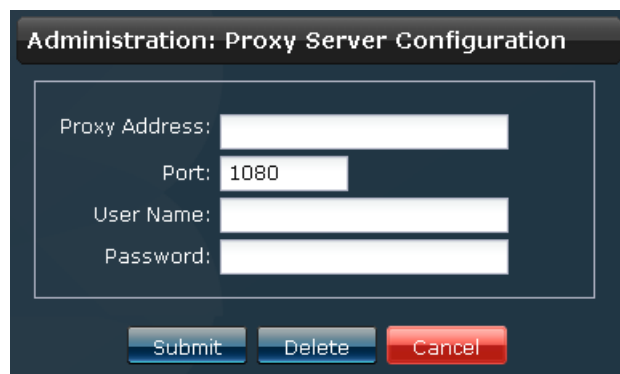
You can configure Service Now to work with a proxy server. When you connect to a proxy server, all communication to and from JSS happens through the proxy server. Both SOCKS and HTTP proxies are supported in Service Now.

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

To configure the proxy server settings:

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

The **Administration: Proxy Server Configuration** dialog box is displayed.

The image shows a dialog box titled "Administration: Proxy Server Configuration". It has a dark blue header bar with the title in white. The main area is white and contains four input fields: "Proxy Address:" with a long text box, "Port:" with a text box containing "1080", "User Name:" with a text box, and "Password:" with a text box. At the bottom, there are three buttons: "Submit" (blue), "Delete" (blue), and "Cancel" (red).

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

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

- Related Topics**
- Configuring Global Settings on page 31
  - Adding an SNMP Server on page 34

## CHAPTER 7

# Service Now Contract and User Roles

- Service Contract on page 37
- Service Now User Roles on page 38

### Service Contract

---

The **Service Contract** task in Service Now displays the details of the Technical Support Contract you purchase from Juniper Networks. When you log in to Service Now, the Service Now Notices gadget on the dashboard indicates the status and provides updates about your contract. Until you create a Service Now organization and validate the organization's connection with JSS, Service Now operates in demo mode. In demo mode, Service Now supports a single organization and up to five devices. The connection between Service Now and Juniper Support Services (JSS) is disabled so you cannot create technical support cases.

When you have a valid contract, the Service Now dashboard notifies you of when your contract is due to expire. With a Technical Support contract with the right level of service, you can add multiple devices and organizations, and upload incidents and iJMBs to JSS for support. To use Service Now you require J-Care Efficiency or Continuity or Agility levels of service.



**NOTE:** If at any point in time, the configured Site ID is invalid, you can continue to use Service Now normally, but the processing of JMBs by JSS fails.

When your support contract expires, Service Now operates in a 60-day grace period. The features supported in the licensed mode is supported in the grace period as well; however, while processing incidents and iJMBs, you receive warnings and the Service Now dashboard also displays the following message:

**Service Contract has expired: Remaining grace period is XX days.**

After the grace period expires, information messages are not processed in JSS. However, incidents are processed.

To view the service contract details, and to check the status of your contract:

1. From the Service Now task ribbon, select **Administration > Service Contract**.

The **Service Contract** page displays the details of the contract. See Table 6 on page 38 for a description of the **Service Contract** page fields.

**Administration: Service Contract**

**Organization:** TEST

**Service Level:** CONTINUITY\_SERVICES

**Service Type:** PARTNER\_SERVICES

**Start Date:** Jan 1, 2009 1:30:00 PM IST

**End Date:** Oct 9, 2009 12:30:00 PM IST

**Last Verified:** May 19, 2010 12:06:26 PM IST

[Refresh Contract](#) [Close](#)

2. Click **Close** to return to the **Global Setting** page.

**Table 6: Service Contract Page Field Description**

Field Name	Description
Organization	Name of customer or partner holding the appropriate Juniper Technical Support Contract.
Service Level	Level of service that is offered —Efficiency Services, Continuity Services, Agility Services, Agility LTD Services.
Service Type	Type of support services that are purchased, which is directly from Juniper Networks or through a Juniper Networks partner.
Start Date	Date and time when the contract period begins.
End Date	Date and time when the contract period expires.
Last Verified	Most recent date when the contract was verified.

**Related Topics** • [Administration Overview on page 1](#)

## Service Now User Roles

The Junos Space User Administrator creates users and assigns roles (permissions) that allow you to access and perform different tasks. You cannot view the tasks that you do not have access to. While Junos Space enables you to create users with custom permissions, it also has a set of predefined user roles. You cannot modify or delete these predefined roles. See Table 7 on page 39, which describes the tasks that predefined Service Now users have access to, based on the roles assigned to them.

You can create users and manage them on the **Manage Users** page, if you have User Administrator permissions. To create and manage these users, select **Application Switcher > Network Application Platform > Users > Manage Users**. The **Manage Users** page lists the existing users. Use this page to create and assign roles to Service Now users.

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

**Table 7: Predefined Service Now User Roles and Permissions**

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

Incidents can be flagged or assigned only to a Service Now Admin or Service Now Unrestricted User. An information message or iJMB can be flagged or assigned to any user. Every user has the ability to clear a flag of an incident or information message that was flagged to that user.

**Related Topics** • [Administration Overview on page 1](#)



## CHAPTER 8

# Index

- Index on page 43



# Index

## A

adding devices.....	21
ai-script	
install.....	22
uninstall.....	25

## D

deleting	
device.....	26
device group.....	17
organization.....	11
device	
associate with device group.....	26
device group	
create.....	15
modify.....	16

## E

export device data	
CSV/excel.....	25

## G

global settings	
global.....	31
proxy server.....	36
snmp server	
add .....	34
edit/delete.....	35

## O

organization	
add.....	7
modify.....	10
run in test mode.....	13
test connection to JSS.....	12
overview	
administration.....	1
ai-scripts.....	27
device groups.....	15

devices.....	19
organization.....	5

## S

script bundle	
add.....	28
delete.....	29
service contract.....	37

## U

user roles.....	38
-----------------	----

