



---

## Junos<sup>®</sup> Space

### Junos<sup>®</sup> Space RESTful Developer Reference for Security Director

Release

13.3R2



---

Modified: 2016-06-24

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

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

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

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

*Junos® Space RESTful Developer Reference for Security Director*

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

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

#### YEAR 2000 NOTICE

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

#### END USER LICENSE AGREEMENT

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

# Table of Contents

	About the Documentation . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Documentation Conventions . . . . .	ix
	Documentation Feedback . . . . .	xi
	Requesting Technical Support . . . . .	xii
	Self-Help Online Tools and Resources . . . . .	xii
	Opening a Case with JTAC . . . . .	xii
<b>Part 1</b>	<b>Security Director RESTful Web Services Overview</b>	
<b>Chapter 1</b>	<b>Security Director RESTful Web Services Overview . . . . .</b>	<b>3</b>
	Security Director RESTful Web Services Overview . . . . .	3
	Using Security Director RESTful Web Services . . . . .	5
	Format and Conventions . . . . .	5
	Media Types . . . . .	5
<b>Part 2</b>	<b>Security Director Objects</b>	
<b>Chapter 2</b>	<b>Address Management RESTful Web Services . . . . .</b>	<b>9</b>
	Address Management RESTful Web Services . . . . .	9
	GET . . . . .	9
	POST . . . . .	13
	PUT . . . . .	14
	DELETE . . . . .	15
	PATCH . . . . .	15
<b>Chapter 3</b>	<b>Service Management RESTful Web Services . . . . .</b>	<b>17</b>
	Service Management RESTful Web Services . . . . .	17
	GET . . . . .	17
	POST . . . . .	24
	PUT . . . . .	25
	DELETE . . . . .	26
	PATCH . . . . .	26
<b>Chapter 4</b>	<b>Application Signature Management RESTful Web Services . . . . .</b>	<b>29</b>
	Application Signature Management RESTful Web Services . . . . .	29
	GET . . . . .	29
	POST . . . . .	33
	PUT . . . . .	37
	DELETE . . . . .	38

<b>Chapter 5</b>	<b>IPS Management RESTful Web Services</b>	<b>41</b>
	IPS Management RESTful Web Services	41
	GET	41
<b>Chapter 6</b>	<b>Variables Management RESTful Web Services</b>	<b>43</b>
	Variables Management RESTful Web Services	43
	GET	43
	POST	46
	PUT	48
	DELETE	49
	PATCH	49
<b>Chapter 7</b>	<b>Scheduler Management RESTful Web Services</b>	<b>51</b>
	Scheduler Management RESTful Web Services	51
	GET	51
	POST	53
	Modify a Scheduler	54
	DELETE	55
<b>Chapter 8</b>	<b>UTM Management RESTful Web Services</b>	<b>57</b>
	UTM Policy Management RESTful Web Services	57
	GET	57
	POST	59
	PUT	60
	DELETE	61
	Antispam Profile Management RESTful Web Services	62
	GET	62
	POST	63
	PUT	63
	DELETE	64
	Antivirus Profile Management RESTful Web Services	64
	GET	64
	POST	66
	PUT	67
	DELETE	68
	Content Filtering Profile Management RESTful Web Services	68
	GET	68
	POST	70
	PUT	71
	DELETE	73
	Web Filtering Profile Management RESTful Web Services	73
	GET	73
	POST	75
	PUT	76
	DELETE	77
	PATCH	77
	URL Pattern Management RESTful Web Services	78
	GET	78
	POST	79
	PUT	80

	DELETE .....	80
	PATCH .....	81
	URL Category Management RESTful Web Services .....	81
	GET .....	81
	POST .....	83
	PUT .....	83
	DELETE .....	84
	PATCH .....	84
	Device Profile Management RESTful Web Services .....	85
	GET .....	85
	POST .....	86
	PUT .....	88
	DELETE .....	89
<b>Chapter 9</b>	<b>Zone Set Management RESTful Web Services .....</b>	<b>91</b>
	Zone Set Management RESTful Web Services .....	91
	POST .....	91
	PUT .....	92
	DELETE .....	92
<b>Part 3</b>	<b>Security Director Services</b>	
<b>Chapter 10</b>	<b>Firewall Policy Management RESTful Web Services .....</b>	<b>95</b>
	Firewall Policy Management RESTful Web Services .....	95
	Firewall Policies .....	95
	GET .....	95
	POST .....	105
	PUT .....	122
	DELETE .....	123
	Policy Profiles .....	124
	GET .....	124
	POST .....	125
	PUT .....	126
	DELETE .....	127
	PATCH .....	127
<b>Chapter 11</b>	<b>VPN Management RESTful Web Services .....</b>	<b>129</b>
	VPN Management RESTful Web Services .....	129
	IPsec VPN .....	129
	GET .....	129
	POST .....	134
	DELETE .....	140
	Extranet Devices .....	140
	GET .....	140
	POST .....	141
	PUT .....	142
	PATCH .....	143
	DELETE .....	144

	VPN Profiles .....	144
	GET .....	144
	POST .....	146
	PUT .....	148
	PATCH .....	149
	DELETE .....	150
<b>Part 4</b>	<b>Security Device Management</b>	
<b>Chapter 12</b>	<b>Device Management RESTful Web Services .....</b>	<b>153</b>
	Device Management RESTful Web Services .....	153
	GET .....	153
	POST .....	157
<b>Part 5</b>	<b>Security Director Job Management</b>	
<b>Chapter 13</b>	<b>Job Management RESTful Web Services .....</b>	<b>163</b>
	Job Management RESTful Web Services .....	163
	GET .....	163

# List of Tables

	<b>About the Documentation . . . . .</b>	<b>ix</b>
	Table 1: Notice Icons . . . . .	x
	Table 2: Text and Syntax Conventions . . . . .	x
<b>Part 1</b>	<b>Security Director RESTful Web Services Overview</b>	
<b>Chapter 1</b>	<b>Security Director RESTful Web Services Overview . . . . .</b>	<b>3</b>
	Table 3: Media-Type String Format Parameters . . . . .	6





# About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

## Documentation and Release Notes

---

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

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

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

## Documentation Conventions

---

Table 1 on page x 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 x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

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

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

## Documentation Feedback

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

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

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

## Requesting Technical Support

---

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

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

## Self-Help Online Tools and Resources

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

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

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

## Opening a Case with JTAC

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

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

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



## PART 1

# Security Director RESTful Web Services Overview

- [Security Director RESTful Web Services Overview on page 3](#)





## CHAPTER 1

# Security Director RESTful Web Services Overview

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

## Security Director RESTful Web Services Overview

---

Security Director RESTful Web Services provide programmatic access to the resources that are defined in Junos Space Security Director. Security Director RESTful Web Services follow the same standards and conventions as the Junos Space Platform RESTful Web Services. The Security Director RESTful Web Services are exposed under the Juniper Networks Junos Space RESTful Web Services root URI (/api). Security Director-related RESTful Web Services are exposed under the /api/juniper/sd URI.

The following RESTful Web Services are exposed under the Junos Space Security Director root URI:

- Address management
- Service management
- Firewall policy management
- Application signature management
- Device management
- IPS management
- Job management
- Variable management
- VPN management
- UTM management

URI: /api/juniper/sd

### Sample XML Output

```
<space>
<services>
  <service rel="info" href="/api/info"/>
  <service rel="sd" href="/api/juniper/sd"/>
```

```

<service rel="address-management" href="/api/juniper/sd/address-management"/>

<service rel="app-sig-management" href="/api/juniper/sd/app-sig-management"/>

<service rel="device-management" href="/api/juniper/sd/device-management"/>
<service rel="fwpolicy-management" href="/api/juniper/sd/fwpolicy-management"/>

<service rel="ips-management" href="/api/juniper/sd/ips-management"/>
<service rel="job-management" href="/api/juniper/sd/job-management"/>
<service rel="scheduler-management"
href="/api/juniper/sd/scheduler-management"/>
<service rel="service-management" href="/api/juniper/sd/service-management"/>
<service rel="utm-management" href="/api/juniper/sd/utm-management"/>
<service rel="variable-management" href="/api/juniper/sd/variable-management"/>

<service rel="vpn-management" href="/api/juniper/sd/vpn-management"/>
</services>
</space>

```

You can get the basic information such as Content-Type and URI for each RESTful Web services. The following example shows getting basic information for Firewall Management RESTful Web Services.

URI: /api/info?uri=/api/juniper/sd/fwpolicy-management/firewall-policies

#### Sample Output

```

<XRD>
<Subject>/api/juniper/sd/fwpolicy-management/firewall-policies</Subject>
<Link rel="describedBy" type="application/xrd+xml"
href="/api/info?type=vnd.juniper.sd.fwpolicy-management.firewall-policy"/>
<http-methods>
<http-method type="POST">
<primary-uri>/api/juniper/sd/fwpolicy-management/firewall-policies</primary-uri>
<query-parameters/>
<headers>
<header type="Accept">
<Link rel="describedBy" type="application/xrd+xml"
href="/api/info?type=vnd.juniper.sd.fwpolicy-management.firewall-policy"/>
<representations>
<representation>application/
vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1;q=0.01
</representation>
<representation>application/
vnd.juniper.sd.fwpolicy-management.firewall-policy+xml;version=1;q=0.01
</representation>
</representations>
</header>
<header type="Content-Type">
<Link rel="describedBy" type="application/xrd+xml"
href="/api/info?type=vnd.juniper.sd.fwpolicy-management.firewall-policy"/>
<representations>
<representation>application/
vnd.juniper.sd.fwpolicy-management.firewall-policy+xml;version=1;charset=UTF-8
</representation>
<representation>application/
vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1;charset=UTF-8
</representation>

```

```

</representations>
</header>
</headers>
</http-method>
<http-method type="GET">
<primary-uri>/api/juniper/sd/fwpolicy-management/firewall-policies</primary-uri>
<query-parameters/>
<headers>
<header type="Accept">
<Link rel="describedBy" type="application/xrd+xml"
href="/api/info?type=vnd.juniper.sd.fwpolicy-management.firewall-policies"/>
<representations>
<representation>application/
vnd.juniper.sd.fwpolicy-management.firewall-policies+json;version=1;q=0.01
</representation>
<representation>application/
vnd.juniper.sd.fwpolicy-management.firewall-policies+xml;version=1;q=0.01
</representation>
</representations>
</header>
</headers>
</http-method>
</http-methods>
</XRD>

```

**Related Documentation**

- [Using Security Director RESTful Web Services on page 5](#)

## Using Security Director RESTful Web Services

- [Format and Conventions on page 5](#)

### Format and Conventions

#### Media Types

Junos Space uses custom media types to define objects that are accessible as HTTP resources and valid targets to HTTP methods, such as GET, PUT, POST, DELETE, and PATCH. For each media type, Junos Space encodes three primary pieces of information about the resources on the wire representation: type, syntax, and version.

#### **Media-Type String Format**

Custom media types defined for Junos Space applications must have the following specified format:

```
application/<vendor>.sd.<service>.<type>+<syntax>;version=<version>
```

For example, Security Director custom media types have the following format:

```
application/vnd.juniper.sd.service-management.services+xml;version="1"
```

[Table 3 on page 6](#) describes these parameters.

Table 3: Media-Type String Format Parameters

Parameter	Description
<vendor>	Vendor of the media type. Media types defined by Juniper Networks use vnd.net.juniper. Third parties must use their own vendor string in the event that they want to define their own Web services in their applications that are deployed on Junos Space.
<service>	Name of the Junos Space-specific service. Service names are all lowercase alphanumeric tokens with hyphen separators.
<type>	Type of resource. Types are all lowercase alphanumeric tokens with hyphen separators.
<syntax>	Representation of the resource.
<version>	Version of the API; versions begin with the numeral 1.



**NOTE:** All the PUT requests must provide the edit version in the HTTP body. The *edit-version* is a mandatory field. The value provided for the *edit-version* field must match the current edit version that you receive by using the GET by ID URI.

**Related  
Documentation**

- [Security Director RESTful Web Services Overview on page 3](#)

## PART 2

# Security Director Objects

- [Address Management RESTful Web Services on page 9](#)
- [Service Management RESTful Web Services on page 17](#)
- [Application Signature Management RESTful Web Services on page 29](#)
- [IPS Management RESTful Web Services on page 41](#)
- [Variables Management RESTful Web Services on page 43](#)
- [Scheduler Management RESTful Web Services on page 51](#)
- [UTM Management RESTful Web Services on page 57](#)
- [Zone Set Management RESTful Web Services on page 91](#)



## CHAPTER 2

# Address Management RESTful Web Services

- [Address Management RESTful Web Services on page 9](#)

## Address Management RESTful Web Services

---

The following operations can be performed using the Security Director Address Management RESTful Web Services.

### GET

This request is used to collect all the address objects that are configured in Security Director.

URI	/api/juniper/sd/address-management/addresses
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.address-management.address-refs+xml;version="1" application/vnd.juniper.sd.address-management.address-refs+JSON;version=1;q=0.01
Consumes	None
Produces	Collection of address objects

### Sample Address Management Output

#### Sample XML Output

```
<addresses total="12" uri="/api/juniper/sd/address-management/addresses">
  <address href="/api/juniper/sd/address-management/addresses/98932"
uri="/api/juniper/sd/address-management/addresses/98932">
    <name>Any</name>
    <address-type>ANY</address-type>
    <description>Predefined any address</description>
    <host-name>
</host-name>
    <domain-id>1</domain-id>
    <id>98932</id>
  </address>
  <address href="/api/juniper/sd/address-management/addresses/98933"
```

```

uri="/api/juniper/sd/address-management/addresses/98933">
  <name>Any-IPv4</name>
  <address-type>ANY_IPV4</address-type>
  <description>Predefined any-ipv4 address</description>
  <host-name>
  </host-name>
  <domain-id>1</domain-id>
  <id>98933</id>
</address>
<address href="/api/juniper/sd/address-management/addresses/98934"
uri="/api/juniper/sd/address-management/addresses/98934">
  <name>Any-IPv6</name>
  <address-type>ANY_IPV6</address-type>
  <description>Predefined any-ipv6 address</description>
  <host-name>
  </host-name>
  <domain-id>1</domain-id>
  <id>98934</id>
</address>
</addresses>

```

**Sample JSON Output**

```

{
  "addresses": {
    "@total": "3",
    "@uri": "/api/juniper/sd/address-management/addresses/",
    "address": [
      {
        "@href": "/api/juniper/sd/address-management/addresses/98932",
        "@uri": "/api/juniper/sd/address-management/addresses/98932",
        "name": "Any",
        "address-type": "ANY",
        "description": "Predefined any address",
        "host-name": "",
        "id": 98932
      },
      {
        "@href": "/api/juniper/sd/address-management/addresses/98933",
        "@uri": "/api/juniper/sd/address-management/addresses/98933",
        "name": "Any-IPv4",
        "address-type": "ANY_IPV4",
        "description": "Predefined any-ipv4 address",
        "host-name": "",
        "id": 98933
      },
      {
        "@href": "/api/juniper/sd/address-management/addresses/98934",
        "@uri": "/api/juniper/sd/address-management/addresses/98934",
        "name": "Any-IPv6",
        "address-type": "ANY_IPV6",
        "description": "Predefined any-ipv6 address",
        "host-name": "",
        "id": 98934
      }
    ]
  }
}

```



### Sample Address Management input and output to get address by ID

URI: /api/juniper/sd/address-management/addresses/98933

This API lists detailed information of the address mentioned in the address ID field. If it is an address-group, the API returns the list of member addresses part of this address group.

#### Sample XML Output

```
<address uri="/api/juniper/sd/address-management/addresses/98933">
  <name>Any-IPv4</name>
  <edit-version>0</edit-version>
  <members uri="/api/juniper/sd/address-management/addresses/98933/members"/>

  <address-type>ANY_IPV4</address-type>
  <description>Predefined any-ipv4 address</description>
  <host-name>
</host-name>
  <address-version>IPv4</address-version>
  <definition-type>PREDEFINED</definition-type>
  <created-by-user-name>Juniper Networks Inc.</created-by-user-name>
  <created-time>2013-04-23T02:31:35Z</created-time>
  <last-modified-time>2013-04-23T02:31:35Z</last-modified-time>
  <domain-id>1</domain-id>
  <id>98933</id>
</address>
```

#### Sample JSON Output

```
{
  "address": {
    "@uri": "/api/juniper/sd/address-management/addresses/6991",
    "addressType": "Wildcard",
    "addressVersion": "IPv4",
    "createdTime": "2012-10-16T05:26:10Z",
    "definitionType": "CUSTOM",
    "description": "WildCard Address",
    "id": 6991,
    "ipAddress": "192.168.0.11/255.255.0.255",
    "lastModifiedTime": "2012-10-16T05:26:10Z",
    "name": "Wildcard_1"
  }
}
```

### Sample Address Management input and output with Pagination

URI: /api/juniper/sd/address-management/addresses?paging=(limit eq 10)      The first 10 addresses in the first page are listed.

URI: /api/juniper/sd/address-management/addresses?paging=(start eq 5, limit eq 10)      Starting from record 5, next 10 records are fetched.

### Sample Address Management Input and Output with Filtering

URI: /api/juniper/sd/address-management/addresses?filter=(global eq 'vpn')

This address search is similar to the address search in the Security Director addresses page. All address names matching with *vpn* are listed.

**Sample XML Output**

```
<addresses total="8" uri="/api/juniper/sd/address-management/addresses">
  <address href="/api/juniper/sd/address-management/addresses/655616"
uri="/api/juniper/sd/address-management/addresses/655616">
    <name>VPN_AD1</name>
    <address-type>IPADDRESS</address-type>
    <ip-address>192.0.2.0</ip-address>
    <description>First Address</description>
    <id>655616</id>
  </address>
  <address href="/api/juniper/sd/address-management/addresses/655617"
uri="/api/juniper/sd/address-management/addresses/655617">
    <name>VPN_AD2</name>
    <address-type>IPADDRESS</address-type>
    <ip-address>192.0.2.1</ip-address>
    <description>Second Address</description>
    <id>655617</id>
  </address>
  <address href="/api/juniper/sd/address-management/addresses/655618"
uri="/api/juniper/sd/address-management/addresses/655618">
    <name>VPN_AD3</name>
    <address-type>IPADDRESS</address-type>
    <ip-address>192.0.2.2</ip-address>
    <description>Third Address</description>
    <id>655618</id>
  </address>
</addresses>
```

URI: /api/juniper/sd/address-management/addresses?filter=(global eq '192.0.2.0') to  
list addresses have IP address 192.0.2.0

**Sample XML Output**

```
<addresses total="1" uri="/api/juniper/sd/address-management/addresses">
  <address href="/api/juniper/sd/address-management/addresses/655616"
uri="/api/juniper/sd/address-management/addresses/655616">
    <name>VPN_AD1</name>
    <address-type>IPADDRESS</address-type>
    <ip-address>192.0.2.0</ip-address>
    <description>First Address</description>
    <id>655616</id>
  </address>
</addresses>
```

**Sample Address Management Input and Output with Sorting**

URI: /api/juniper/sd/address-management/addresses?sorting=(name(ascending))

This request lists the addresses in an ascending order.

**Sample XML Output**

```
<addresses total="12" uri="/api/juniper/sd/address-management/addresses">
  <address href="/api/juniper/sd/address-management/addresses/98932"
uri="/api/juniper/sd/address-management/addresses/98932">
    <name>Any</name>
    <address-type>ANY</address-type>
    <description>Predefined any address</description>
    <host-name>
    </host-name>
    <id>98932</id>
  </address>
```

```

    <address href="/api/juniper/sd/address-management/addresses/98933"
uri="/api/juniper/sd/address-management/addresses/98933">
    <name>Any-IPv4</name>
    <address-type>ANY_IPV4</address-type>
    <description>Predefined any-ipv4 address</description>
    <host-name>
    </host-name>
    <id>98933</id>
    </address>
    <address href="/api/juniper/sd/address-management/addresses/98934"
uri="/api/juniper/sd/address-management/addresses/98934">
    <name>Any-IPv6</name>
    <address-type>ANY_IPV6</address-type>
    <description>Predefined any-ipv6 address</description>
    <host-name>
    </host-name>
    <id>98934</id>
    </address>
  </addresses>

```

URI: /api/juniper/sd/address-management/addresses?sorting=(name(descending))

This request lists the addresses in a descending order.

## POST

This request is used to create an address. If you are creating an address group, you must create a list of member addresses.

URI	/api/juniper/sd/address-management/addresses
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.address-management.address+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.address-management.address+json;version=1;charset=UTF-8
Consumes	None
Produces	Creates a new address object

To create a new address object:

1. Send the new address object information to the Junos Space server, as shown in the following example. Copy this information in the Body window, and send it to the Junos Space server.

```

<address>
  <name>iXS_AD1</name>
  <address-type>IPADDRESS</address-type>
  <host-name />
  <edit-version />
  <members />
  <address-version>IPV4</address-version>
  <definition-type>CUSTOM</definition-type>

```

```

    <ip-address>198.51.100.1</ip-address>
    <description> A new address</description>
  </address>

```

2. A new address object is created. You can verify the same by querying Security Director to return all address objects.

## PUT

This request is used to modify an address. Because this is a full replace and if it is an address group, all the member addresses must be part of this address group.

URI	/api/juniper/sd/address-management/addresses/{address-id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.address-management.address+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.address-management.address+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies an address object

To modify any address object:

1. Send the modified information to the Junos Space server, as shown in the following example. In this example, edit version value and ID are modified.

### Sample Modified Values

```

<address>
  <name>IX_AD1</name>
  <address-type>IPADDRESS</address-type>
  <host-name />
  <edit-version>0</edit-version>
  <id>32768</id>
  <members />
  <address-version>IPV4</address-version>
  <definition-type>CUSTOM</definition-type>
  <ip-address>198.51.100.1</ip-address>
  <description>desc1</description>
</address>

```

### Sample XML Input After the Modification

```

<address uri="/api/juniper/sd/address-management/addresses/33413">
  <name>IX_AD1</name>
  <edit-version>1</edit-version>
  <members
uri="/api/juniper/sd/address-management/addresses/33413/members"/>
    <address-type>IPADDRESS</address-type>
    <ip-address>198.51.100.1</ip-address>
    <description>desc1</description>
  </members>
</address>

```

```

<host-name>
</host-name>
<address-version>IPv4</address-version>
<definition-type>CUSTOM</definition-type>
<created-time>2013-03-21T08:56:57Z</created-time>
<last-modified-time>2013-03-21T10:20:05.341Z</last-modified-time>
<id>33413</id>
</address>

```

## DELETE

This request is used to delete a particular address.

URI	/api/juniper/sd/address-management/addresses/{address-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.address-management.delete-address-response+xml;version=1;q=0.01 application/vnd.juniper.sd.address-management.delete-address-response+json;version=1;q=0.01
Consumes	None
Produces	Deletes an address object

## PATCH

This request is used to patch or partially modify an address.

URI	/api/juniper/sd/address-management/addresses/{address-id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.address-management.address_patch+xml;version=1;charset=UTF-8
Consumes	None
Produces	Partially modifies an address object

To patch an address:

1. Send the patch information to the Junos Space server, as shown in the following example. Copy this information in the Body window, and send it to the Junos Space server.

### Sample XML Input 1

```

<diff>
  <replace sel="address/name">
    <name>User_AD1_patch</name>
  </replace>
  <replace sel="address/description">

```

```
<description>description modified</description>
</replace>
</diff>
```

#### Sample XML Input to Patch Address Name

```
<diff>
  <replace sel="address/name">
    <name>User_AD1_patch</name>
  </replace>
</diff>
```

#### Sample XML Input to Add Member in the existing address group

```
<diff>
  <add sel="address/members">
    <member>
      <id/>
      <name>10.128.1.26_FOHP</name>
    </member>
  </add>
</diff>
```

#### Sample XML Input

```
<diff>
  <remove sel="address/members/member[name='User_AD_Group3']"/>
</diff>
```

2. The partially modified address information can be viewed in the device.

#### Related Documentation

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

CHAPTER 3

# Service Management RESTful Web Services

- [Service Management RESTful Web Services on page 17](#)

## Service Management RESTful Web Services

The following operations can be performed using the Security Director Service Management RESTful Web Services.

### GET

This request is used collect all the service-management services and their associated parameters that are configured in Security Director.

URI	api/juniper/sd/service-management/services
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.service-management.services+xml;version=1;q=0.01 application/vnd.juniper.sd.service-management.services+json;version=1;q=0.01
Consumes	None
Produces	Collection of services

### Sample Service Management Output

Sample XML Output

```
<services total="223" uri="/api/juniper/sd/service-management/services">
  <service href="/api/juniper/sd/service-management/services/98304"
uri="/api/juniper/sd/service-management/services/98304">
    <id>98304</id>
    <name>Any</name>
    <description>predefined any service</description>
    <is-group>>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98305"
uri="/api/juniper/sd/service-management/services/98305">
    <id>98305</id>
    <name>ftp</name>
```

```
<description>predefined service</description>
<is-group>false</is-group>
</service>
<service href="/api/juniper/sd/service-management/services/98307"
uri="/api/juniper/sd/service-management/services/98307">
  <id>98307</id>
  <name>tftp</name>
  <description>predefined service</description>
  <is-group>false</is-group>
</service>
<service href="/api/juniper/sd/service-management/services/98309"
uri="/api/juniper/sd/service-management/services/98309">
  <id>98309</id>
  <name>rtsp</name>
  <description>predefined service</description>
  <is-group>false</is-group>
</service>
<service href="/api/juniper/sd/service-management/services/98311"
uri="/api/juniper/sd/service-management/services/98311">
  <id>98311</id>
  <name>netbios-session</name>
  <description>predefined service</description>
  <is-group>false</is-group>
</service>
.
.
.
.
<service href="/api/juniper/sd/service-management/services/99014"
uri="/api/juniper/sd/service-management/services/99014">
  <id>99014</id>
  <name>sun-rpc-any</name>
  <description>
  </description>
  <is-group>true</is-group>
</service>
</services>
```

**Sample JSON Output**

```
{
  "services": {
    "@total": "199",
    "@uri": "/api/juniper/sd/service-management/services",
    "service": [
      {
        "@href": "/api/juniper/sd/service-management/services/98304",
        "@uri": "/api/juniper/sd/service-management/services/98304",
        "id": 98304,
        "name": "Any",
        "description": "predefined any service",
        "is-group": false
      },
      {
        "@href": "/api/juniper/sd/service-management/services/98305",
        "@uri": "/api/juniper/sd/service-management/services/98305",
        "id": 98305,
        "name": "ftp",
```



```

    "description": "predefined service",
    "is-group": false
  },
  {
    "@href": "/api/juniper/sd/service-management/services/98965",
    "@uri": "/api/juniper/sd/service-management/services/98965",
    "id": 98965,
    "name": "ms-rpc-any",
    "description": "",
    "is-group": true
  }
]
}
}

```

### Sample Service Management Input and Output to get service by ID

URI: /api/juniper/sd/service-management/services/98307

This API will give more information of the service mentioned in the service ID field.

#### Sample XML Output

```

<service href="/api/juniper/sd/service-management/services/98307"
uri="/api/juniper/sd/service-management/services/98307">
  <last-modified-time>2013-04-23T02:30:58Z</last-modified-time>
  <id>98307</id>
  <created-time>2013-04-23T02:30:58Z</created-time>
  <created-by-user-name>Juniper Networks Inc.</created-by-user-name>
  <protocols>
    <protocol>
      <sunrpc-protocol-type>17</sunrpc-protocol-type>
      <msrpc-protocol-type>17</msrpc-protocol-type>
      <protocol-number>17</protocol-number>
      <name>tftp</name>
      <alg>tftp</alg>
      <dst-port>69</dst-port>
      <disable-timeout>>false</disable-timeout>
      <protocol-type>1</protocol-type>
      <rpc-program-number>0</rpc-program-number>
      <icmp-code>0</icmp-code>
      <icmp-type>0</icmp-type>
    </protocol>
  </protocols>
  <edit-version>0</edit-version>
  <name>tftp</name>
  <is-group>>false</is-group>
  <description>predefined service</description>
  <members total="0"
uri="/api/juniper/sd/service-management/services/98307/members"/>
</service>

```

#### Sample JSON Output

```

{
  "service": {
    "@uri": "/api/juniper/sd/service-management/services/6954",
    "createdTime": "2012-10-16T05:26:09Z",
    "description": "User predefined application",
    "id": 6954,

```

```
"lastModifiedTime": "2012-10-16T05:26:09Z",
"name": "App4_SUN-RPC",
"protocols": [
  {
    "name": "one_sun",
    "protocolNumber": 17,
    "protocolType": "SUN-RPC",
    "rpcProgramNumber": 123,
    "sunrpcProtocolType": 17
  },
  {
    "name": "two_sun",
    "protocolNumber": 6,
    "protocolType": "SUN-RPC",
    "rpcProgramNumber": 124,
    "sunrpcProtocolType": 6
  }
]
}
```

#### Sample Service Management Input and Output with Pagination

URL: /api/juniper/sd/service-management/services?paging=(start eq 10, limit eq 5)

The input parameters to this API are the record number and the number of records to display in each page.

#### Sample XML Output

```
<services total="223" uri="/api/juniper/sd/service-management/services">
  <service href="/api/juniper/sd/service-management/services/98323"
    uri="/api/juniper/sd/service-management/services/98323">
    <id>98323</id>
    <name>dhcp-client</name>
    <description>predefined service</description>
    <is-group>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98325"
    uri="/api/juniper/sd/service-management/services/98325">
    <id>98325</id>
    <name>dhcp-server</name>
    <description>predefined service</description>
    <is-group>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98327"
    uri="/api/juniper/sd/service-management/services/98327">
    <id>98327</id>
    <name>bootpc</name>
    <description>predefined service</description>
    <is-group>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98329"
    uri="/api/juniper/sd/service-management/services/98329">
    <id>98329</id>
    <name>bootps</name>
    <description>predefined service</description>
    <is-group>false</is-group>
  </service>
</services>
```

```

</service>
<service href="/api/juniper/sd/service-management/services/98331"
uri="/api/juniper/sd/service-management/services/98331">
  <id>98331</id>
  <name>finger</name>
  <description>predefined service</description>
  <is-group>false</is-group>
</service>
</services>

```

#### Sample JSON Ouput

```

{
  "services": {
    "@total": "223",
    "@uri": "/api/juniper/sd/service-management/services",
    "service": [
      {
        "@href": "/api/juniper/sd/service-management/services/98323",
        "@uri": "/api/juniper/sd/service-management/services/98323",
        "id": 98323,
        "name": "dhcp-client",
        "description": "predefined service",
        "is-group": false
      },
      {
        "@href": "/api/juniper/sd/service-management/services/98325",
        "@uri": "/api/juniper/sd/service-management/services/98325",
        "id": 98325,
        "name": "dhcp-server",
        "description": "predefined service",
        "is-group": false
      },
      {
        "@href": "/api/juniper/sd/service-management/services/98327",
        "@uri": "/api/juniper/sd/service-management/services/98327",
        "id": 98327,
        "name": "bootpc",
        "description": "predefined service",
        "is-group": false
      },
      {
        "@href": "/api/juniper/sd/service-management/services/98329",
        "@uri": "/api/juniper/sd/service-management/services/98329",
        "id": 98329,
        "name": "bootps",
        "description": "predefined service",
        "is-group": false
      },
      {
        "@href": "/api/juniper/sd/service-management/services/98331",
        "@uri": "/api/juniper/sd/service-management/services/98331",
        "id": 98331,
        "name": "finger",
        "description": "predefined service",
        "is-group": false
      }
    ]
  }
}

```

```
}
}
```

URI: /api/juniper/sd/service-management/services?paging=(limit eq 10) displays only 10 records from the first page.

### Sample Service Management Input and Output with Filtering

URI: /api/juniper/sd/service-management/services?filter=(global eq 'smtp')

This Service search is similar to the service search in the Security Director Services page. All the GUI search support is available using this API.

#### Sample XML Output

```
<services total="1" uri="/api/juniper/sd/service-management/services">
  <service href="/api/juniper/sd/service-management/services/98317"
uri="/api/juniper/sd/service-management/services/98317">
    <id>98317</id>
    <name>smtp</name>
    <description>predefined service</description>
    <is-group>false</is-group>
  </service>
</services>
```

#### Sample JSON Output

```
{
  "services": {
    "@total": "1",
    "@uri": "/api/juniper/sd/service-management/services",
    "service": {
      "@href": "/api/juniper/sd/service-management/services/98317",
      "@uri": "/api/juniper/sd/service-management/services/98317",
      "id": 98317,
      "name": "smtp",
      "description": "predefined service",
      "is-group": false
    }
  }
}
```

### Sample Service Management Input and Output with Sorting

URI: /api/juniper/sd/service-management/services?sortby=(name(ascending))

Services are listed in an ascending order.

#### Sample XML Output

```
<services total="223" uri="/api/juniper/sd/service-management/services">
  <service href="/api/juniper/sd/service-management/services/98304"
uri="/api/juniper/sd/service-management/services/98304">
    <id>98304</id>
    <name>Any</name>
    <description>predefined any service</description>
    <is-group>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98385"
uri="/api/juniper/sd/service-management/services/98385">
    <id>98385</id>
    <name>aol</name>
```

```

    <description>predefined service</description>
    <is-group>>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98674"
uri="/api/juniper/sd/service-management/services/98674">
    <id>98674</id>
    <name>apple-ichat</name>
    <description>predefined service</description>
    <is-group>>true</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98618"
uri="/api/juniper/sd/service-management/services/98618">
    <id>98618</id>
    <name>apple-ichat-snatmap</name>
    <description>predefined service</description>
    <is-group>>false</is-group>
  </service>

```

URI: /api/juniper/sd/service-management/services?sortBy=(name(descending))

Services are listed in a descending order.

#### Sample XML Output

```

<services total="223" uri="/api/juniper/sd/service-management/services">
  <service href="/api/juniper/sd/service-management/services/98558"
uri="/api/juniper/sd/service-management/services/98558">
    <id>98558</id>
    <name>ymsg</name>
    <description>predefined service</description>
    <is-group>>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98379"
uri="/api/juniper/sd/service-management/services/98379">
    <id>98379</id>
    <name>xnm-ssl</name>
    <description>predefined service</description>
    <is-group>>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98381"
uri="/api/juniper/sd/service-management/services/98381">
    <id>98381</id>
    <name>xnm-clear-text</name>
    <description>predefined service</description>
    <is-group>>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98556"
uri="/api/juniper/sd/service-management/services/98556">
    <id>98556</id>
    <name>x-windows</name>
    <description>predefined service</description>
    <is-group>>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98560"
uri="/api/juniper/sd/service-management/services/98560">
    <id>98560</id>
    <name>wxcontrol</name>
    <description>predefined service</description>

```

```

    <is-group>false</is-group>
  </service>
  <service href="/api/juniper/sd/service-management/services/98554"
uri="/api/juniper/sd/service-management/services/98554">
    <id>98554</id>
    <name>winframe</name>
    <description>predefined service</description>
    <is-group>false</is-group>
  </service>

```

## POST

This request is used to create a new service.

URI	/api/juniper/sd/service-management/services
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.service-management.service+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.service-management.service+json;version=1;charset=UTF-8
Consumes	None
Produces	Creates a new service

To create a new service:

1. Send the new service information to the device, as shown in the following example. Copy this information in Body window, and send to the device.

```

<service>
  <name>App1</name>
  <created-by-user-name />
  <edit-version />
  <id />
  <description>predefined application</description>
  <is-group>false</is-group>
  <domain-id>0</domain-id>
  <members />
  <protocols>
    <protocol>
      <name>one</name>
      <sunrpc-protocol-type>6</sunrpc-protocol-type>
      <msrpc-protocol-type>6</msrpc-protocol-type>
      <protocol-number>6</protocol-number>
      <dst-port>21</dst-port>
      <disable-timeout>true</disable-timeout>
      <protocol-type>0</protocol-type>
      <rpc-program-number>0</rpc-program-number>
      <icmp-code>0</icmp-code>
      <icmp-type>0</icmp-type>
      <alg>ftp</alg>
    </protocol>
  </protocols>

```

```

<protocol>
  <name>two</name>
  <sunrpc-protocol-type>6</sunrpc-protocol-type>
  <msrpc-protocol-type>6</msrpc-protocol-type>
  <protocol-number>6</protocol-number>
  <dst-port>100</dst-port>
  <disable-timeout>true</disable-timeout>
  <protocol-type>0</protocol-type>
  <rpc-program-number>0</rpc-program-number>
  <icmp-code>0</icmp-code>
  <icmp-type>0</icmp-type>
  <alg>ftp</alg>
</protocol>
</protocols>
</service>

```

2. A new service is created.

## PUT

This request is used to modify a service.

URI	/api/juniper/sd/service-management/services/{service-id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.service-management.service+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.service-management.service+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies any service

To modify any service

1. Send the modification information to the device, by copying the information in the Body window. In the following example, edit version and ID are modified.

```

<service>
  <name>App1</name>
  <created-by-user-name />
  <edit-version >1</edit-version/>
  <id>333 </id>
  <description>predefined application</description>
  <is-group>false</is-group>
  <domain-id>0</domain-id>
  <members />
  <protocols>
    <protocol>
      <name>one</name>
      <sunrpc-protocol-type>6</sunrpc-protocol-type>
      <msrpc-protocol-type>6</msrpc-protocol-type>
      <protocol-number>6</protocol-number>
    
```

```

<dst-port>21</dst-port>
<disable-timeout>true</disable-timeout>
<protocol-type>0</protocol-type>
<rpc-program-number>0</rpc-program-number>
<icmp-code>0</icmp-code>
<icmp-type>0</icmp-type>
<alg>ftp</alg>
</protocol>
<protocol>
<name>two</name>
<sunrpc-protocol-type>6</sunrpc-protocol-type>
<msrpc-protocol-type>6</msrpc-protocol-type>
<protocol-number>6</protocol-number>
<dst-port>100</dst-port>
<disable-timeout>true</disable-timeout>
<protocol-type>0</protocol-type>
<rpc-program-number>0</rpc-program-number>
<icmp-code>0</icmp-code>
<icmp-type>0</icmp-type>
<alg>ftp</alg>
</protocol>
</protocols>
</service>

```

2. Required fields are modified in a service.

## DELETE

This request is used to delete a service.

URI	/api/juniper/sd/service-management/services/{service-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.service-management.service+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.service-management.service+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes a service

## PATCH

This request is used to patch or partially modify a service.

URI	/api/juniper/sd/service-management/services/{service-id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.service-management.service_patch+xml;version=1;charset=UTF-8
Consumes	None



Produces

Patches a service

To patch a service:

1. Send the patch information to the device, as shown in the following example. Copy this information in the Body window, and send it to the device.

#### Sample XML Input 1

```
<!--App_TCP-->
<diff>
  <replace sel="application/name">
    <name>App_TCP_patch</name>
  </replace>
</diff>
```

#### Sample XML Input 2

```
<!--App_UDP-->
<diff>
  <replace sel="application/protocols/protocol/name">
    <name>one_sccp_patch</name>
  </replace>
  <replace sel="application/description">
    <description>description modified</description>
  </replace>
</diff>
```

#### Sample XML Input 3

```
<!--App3-->
<diff>
  <add sel="application/protocols/">
    <protocol>
      <sunrpc-protocol-type>17</sunrpc-protocol-type>
      <msrpc-protocol-type>17</msrpc-protocol-type>
      <protocol-number>17</protocol-number>
      <name>sun_rcp_tcp_patch</name>
      <alg>sun-rpc</alg>
      <src-port/>
      <dst-port>121</dst-port>
      <disable-timeout>true</disable-timeout>
      <protocol-type>3</protocol-type>
      <rpc-program-number>14</rpc-program-number>
      <icmp-code>0</icmp-code>
      <icmp-type>0</icmp-type>
      <description/>
    </protocol>
  </add>
</diff>
```

#### Sample XML Input to Add a Service to a Service Group

```
<diff>
  <add sel="service/members">
```

```
<member>
  <name>App_UDP</name>
</member>
</add>
</diff>
```

**Sample XML Input to Remove a Service from the Service Group**

```
<diff>
<remove sel="service/members/member[name='App_Group_1']"/>
</diff>
```

**Sample XML Input to Remove Protocol Term from the Service**

```
<diff>
<remove sel="service/protocols/protocol[name='ms-tcp-pro']"/>
</diff>
```

2. The partial modification is performed for a service.

**Related  
Documentation**

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

CHAPTER 4

# Application Signature Management RESTful Web Services

- [Application Signature Management RESTful Web Services on page 29](#)

## Application Signature Management RESTful Web Services

The following operations can be performed using the Security Director Application Signature Management RESTful Web Services.

### GET

This request is used to get all application signatures configured in Security Director.

URI	/api/juniper/sd/app-sig-management
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.app-sig-management+xml;version="1" application/vnd.juniper.sd.app-sig-management+json;version="1"
Consumes	None
Produces	Collection of application signatures

### Sample Application Signature Management Input and Output to Get All Application Signatures

URI: /api/juniper/sd/app-sig-management/app-sigs

This request is used to get all application signatures. Get all application signatures support paging, sorting by name and global filtering.

**Sample XML output**

```
<app-sigs total="1751" uri="/api/juniper/sd/app-sig-management/app-sigs">
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/361"
uri="/api/juniper/sd/app-sig-management/app-sigs/361">
    <display-name>MISC: Finger Protocol</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>361</id>
    <name>FINGER</name>
```

```

    <type>protocol</type>
    <category>Infrastructure</category>
  </app-sig>
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/363"
uri="/api/juniper/sd/app-sig-management/app-sigs/363">
    <display-name>Infrastructure:Directory</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>363</id>
    <name>Infrastructure:Directory</name>
    <type>group</type>
    <category>Infrastructure</category>
  </app-sig>
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/364"
uri="/api/juniper/sd/app-sig-management/app-sigs/364">
    <display-name>Infrastructure</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>364</id>
    <name>Infrastructure</name>
    <type>group</type>
    <category>Infrastructure</category>
  </app-sig>
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/366"
uri="/api/juniper/sd/app-sig-management/app-sigs/366">
    <display-name>MISC: Echo Protocol</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>366</id>
    <name>ECHO</name>
    <type>protocol</type>
    <category>Infrastructure</category>
  </app-sig>
</app-sigs>

```

### Sample Application Signature Management Input and Output to Get Application Signature by ID

URI: /api/juniper/sd/app-sig-management/app-sigs/361

#### Sample XML Output

```

<app-sig uri="/api/juniper/sd/app-sig-management/app-sigs/361">
  <edit-version>0</edit-version>
  <definition-type>PREDEFINED</definition-type>
  <id>361</id>
  <objtype>0</objtype>
  <display-name>MISC: Finger Protocol</display-name>
  <application-name>FINGER</application-name>
  <disable-state>>false</disable-state>
  <pattern-sets>
    <pattern-set>
      <ctspattern>.+</ctspattern>
      <default-port>TCP/79</default-port>
      <logic-function>
        </logic-function>
      <max-transactions>0</max-transactions>
      <members/>
      <mindata>1</mindata>
      <ordered>>false</ordered>
      <pattern-order>0</pattern-order>
    </pattern-set>
  </pattern-sets>

```

```

    <port>TCP/79</port>
    <stcpattern>.+</stcpattern>
    <type>protocol</type>
    <protocol>HTTP</protocol>
  </pattern-set>
</pattern-sets>
<name>FINGER</name>
<version-no>2255</version-no>
<app-id>8</app-id>
<description>This signature detects the Finger Protocol.</description>
<app-sig-tags>
  <idp-common-value>
    <name>Category</name>
    <value>Infrastructure</value>
  </idp-common-value>
  <idp-common-value>
    <name>Subcategory</name>
    <value>Directory</value>
  </idp-common-value>
  <idp-common-value>
    <name>Characteristic</name>
    <value>Can Leak Information</value>
  </idp-common-value>
  <idp-common-value>
    <name>Characteristic</name>
    <value>Known Vulnerabilities</value>
  </idp-common-value>
  <idp-common-value>
    <name>Risk</name>
    <value>2</value>
  </idp-common-value>
</app-sig-tags>
<urls>
  <url>http://tools.ietf.org/html/rfc1288</url>
</urls>
<type>protocol</type>
<order>5</order>
<chainorder>>false</chainorder>
<group-nested-members total="0"/>
<group-app-members total="0"/>
<max_transactions>0</max_transactions>
<parent-id>0</parent-id>
<default-port>TCP/79</default-port>
<app>
  <protocol-name>FINGER</protocol-name>
  <port>TCP/79</port>
  <appentry>
    <order>0</order>
    <mindata>1</mindata>
  </appentry>
</app>
<category>Infrastructure</category>
<aliases/>
</app-sig>

```

#### Sample Variable Management Input and Output with Sorting

URI: /api/juniper/sd/app-sig-management/app-sigs?sortby=(name (ascending))

This request lists the application signatures in an ascending order.

#### Sample XML Output

```
<app-sigs total="1751" uri="/api/juniper/sd/app-sig-management/app-sigs">
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/361"
uri="/api/juniper/sd/app-sig-management/app-sigs/361">
    <display-name>MISC: Finger Protocol</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>361</id>
    <name>FINGER</name>
    <type>protocol</type>
    <category>Infrastructure</category>
  </app-sig>
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/363"
uri="/api/juniper/sd/app-sig-management/app-sigs/363">
    <display-name>Infrastructure:Directory</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>363</id>
    <name>Infrastructure:Directory</name>
    <type>group</type>
    <category>Infrastructure</category>
  </app-sig>
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/364"
uri="/api/juniper/sd/app-sig-management/app-sigs/364">
    <display-name>Infrastructure</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>364</id>
    <name>Infrastructure</name>
    <type>group</type>
    <category>Infrastructure</category>
  </app-sig>
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/366"
uri="/api/juniper/sd/app-sig-management/app-sigs/366">
    <display-name>MISC: Echo Protocol</display-name>
    <definition-type>PREDEFINED</definition-type>
    <id>366</id>
    <name>ECHO</name>
    <type>protocol</type>
    <category>Infrastructure</category>
  </app-sig>
</app-sigs>
```

URI: /api/juniper/sd/app-sig-management/app-sigs?sortby=(name (descending))

This request lists the application signatures in descending order.

#### Sample Application Signature Management Input and Output with Pagination

URI	Description
/api/juniper/sd/app-sig-management/app-sigs?paging=(limit eq 10)	Ten application signatures are listed
/api/juniper/sd/app-sig-management/app-sigs?paging=(start eq 100, limit eq 10)	From record number 100, ten application signatures are listed.

## POST

This request is to create a new application signature.

URI	/api/juniper/sd/app-sig-management/app-sigs
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.app-sig-management.app-sig+json;version=1;charset=UTF-8 application/vnd.juniper.sd.app-sig-management.app-sig+xml;version=1;charset=UTF-8
Consumes	None
Produces	Creates a new application signature

### Creating a New Application Signature in Basic Mode

#### Sample XML Input

```
<app-sig>
  <pattern-sets>
    <pattern-set>
      <port>TCP/444-9999</port>
      <protocol>HTTP</protocol>
      <stcpattern>
        axkeiepoep
      </stcpattern>
      <mindata>65534</mindata>
      <ordered>>false</ordered>
      <ctspattern>[a-z][A-Z][0-9]*----[0-9]*</ctspattern>
    </pattern-set>
  </pattern-sets>
  <domain-id>3</domain-id>
  <description>
    Automated user - custom signature creation with basic type
  </description>
  <disable-state>>false</disable-state>
  <last-modified-time>2014-05-09T19:52:48+05:30</last-modified-time>
  <name>custBasicAppSig1</name>
  <app-id-version>ALL</app-id-version>
  <device-compatibility>X46_AND_OLDER</device-compatibility>
  <app-sig-tags>
    <idp-common-value>
      <name>Category</name>
      <value>Remote-Access</value>
    </idp-common-value>
    <idp-common-value>
      <name>Subcategory</name>
      <value>Authentication</value>
    </idp-common-value>
    <idp-common-value>
      <name>Characteristic</name>
      <value />
    </idp-common-value>
  </idp-common-value>
</app-sig>
```

```
<name>Risk</name>
<value>5</value>
</idp-common-value>
</app-sig-tags>
<definition-type>CUSTOM</definition-type>
<category>Remote-Access</category>
<chainorder>>false</chainorder>
<domain-name>Global</domain-name>
<application-name>custBasicAppSig1</application-name>
<type>protocol</type>
</app-sig>
```

### Creating a New Application Signature in Advanced Mode

#### Sample XML Input

```
<app-sig>
<pattern-sets>
<pattern-set>
<port>TCP/2430-65520</port>
<max-transactions>1200</max-transactions>
<protocol>HTTP</protocol>
<ordered>>true</ordered>
<members>
<pattern-member>
<pattern-order>0</pattern-order>
<pattern>pattern1</pattern>
<direction>cts</direction>
<context>http-post-url-parsed-param-parsed</context>
</pattern-member>
<pattern-member>
<pattern-order>0</pattern-order>
<pattern>pattern2</pattern>
<direction>stc</direction>
<context>http-header-cookie</context>
</pattern-member>
<pattern-member>
<pattern-order>0</pattern-order>
<pattern>pattern3</pattern>
<direction>cts</direction>
<context>http-header-content-type</context>
</pattern-member>
<pattern-member>
<pattern-order>0</pattern-order>
<pattern>aaaaa\|||||****????</pattern>
<direction>cts</direction>
<context>http-get-url-parsed-param-parsed</context>
</pattern-member>
<pattern-member>
<pattern-order>0</pattern-order>
<pattern>pattern4</pattern>
<direction>stc</direction>
<context>http-header-host</context>
</pattern-member>
<pattern-member>
<pattern-order>0</pattern-order>
<pattern>pattern5</pattern>
<direction>stc</direction>
```



```

    <context>http-header-user-agent</context>
  </pattern-member>
  <pattern-member>
    <pattern-order>0</pattern-order>
    <pattern>pattern6</pattern>
    <direction>cts</direction>
    <context>http-post-variable-parsed</context>
  </pattern-member>
  <pattern-member>
    <pattern-order>0</pattern-order>
    <pattern>pattern6</pattern>
    <direction>stc</direction>
    <context>http-url-parsed</context>
  </pattern-member>
  <pattern-member>
    <pattern-order>0</pattern-order>
    <pattern>pattern7</pattern>
    <direction>cts</direction>
    <context>http-url-parsed-param-parsed</context>
  </pattern-member>
  <pattern-member>
    <pattern-order>0</pattern-order>
    <pattern>pattern7</pattern>
    <direction>cts</direction>
    <context>stream</context>
  </pattern-member>
  <pattern-member>
    <pattern-order>0</pattern-order>
    <pattern>pattern7</pattern>
    <direction>any</direction>
    <context>stream</context>
  </pattern-member>
</members>
</pattern-set>
</pattern-sets>
<domain-id>3</domain-id>
<description>
  Automated user custom application signature creation - with advanced
  signature type
</description>
<disable-state>>false</disable-state>
<name>custAppAdvSig1</name>
<app-id-version>ALL</app-id-version>
<device-compatibility>X46_AND_OLDER</device-compatibility>
<app-sig-tags>
  <idp-common-value>
    <name>Category</name>
    <value>Social-Networking</value>
  </idp-common-value>
  <idp-common-value>
    <name>Subcategory</name>
    <value>Multimedia</value>
  </idp-common-value>
  <idp-common-value>
    <name>Characteristic</name>
    <value />
  </idp-common-value>

```

```

</idp-common-value>
<idp-common-value>
  <name>Risk</name>
  <value>3</value>
</idp-common-value>
</app-sig-tags>
<definition-type>CUSTOM</definition-type>
<category>Social-Networking</category>
<chainorder>>false</chainorder>
<domain-name>Global</domain-name>
<application-name>custAppAdvSig1</application-name>
<type>application</type>
</app-sig>

```

### Creating a Custom Application Signature Group

#### Sample XML Input

```

<app-sig>
  <domain-id>3</domain-id>
  <group-app-members>
    <group-nested-member>
      <disable-state>>false</disable-state>
      <name>custBasicAppSig1</name>
      <domain-name>Global</domain-name>
      <domain-id>3</domain-id>
      <type>protocol</type>
      <chainorder>>false</chainorder>
    </group-nested-member>
    <group-nested-member>
      <disable-state>>false</disable-state>
      <name>custBasicAppSig2</name>
      <domain-name>Global</domain-name>
      <domain-id>3</domain-id>
      <type>protocol</type>
      <chainorder>>false</chainorder>
    </group-nested-member>
  </group-app-members>
  <disable-state>>false</disable-state>
  <created-by-user-name>super</created-by-user-name>
  <name>custAppSigGroup1</name>
  <app-id-version>ALL</app-id-version>
  <device-compatibility>X46_AND_OLDER</device-compatibility>
  <app-sig-tags>
    <idp-common-value>
      <name>Category</name>
      <value />
    </idp-common-value>
    <idp-common-value>
      <name>Subcategory</name>
      <value />
    </idp-common-value>
    <idp-common-value>
      <name>Characteristic</name>
      <value />
    </idp-common-value>
    <idp-common-value>
      <name>Risk</name>

```

```

<value />
</idp-common-value>
</app-sig-tags>
<definition-type>CUSTOM</definition-type>
<category />
<last-modified-by-user-name>super</last-modified-by-user-name>
<chainorder>>false</chainorder>
<domain-name>Global</domain-name>
<application-name>custAppSigGroup1</application-name>
<group-nested-members>
  <group-nested-member>
    <disable-state>>false</disable-state>
    <name>custAppAdvSig1</name>
    <domain-name>Global</domain-name>
    <domain-id>3</domain-id>
    <type>application</type>
    <chainorder>>false</chainorder>
  </group-nested-member>
</group-nested-members>
<type>group</type>
</app-sig>

```

## PUT

This request is to modify the application signature.

URI	/api/juniper/sd/app-sig-management/app-sigs
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.app-sig-management.app-sig+json;version=1;charset=UTF-8 application/vnd.juniper.sd.app-sig-management.app-sig+xml;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the application signature.

To modify an application signature, send the modify information in the Body window as shown in the following example.

### Sample XML Input

```

<app-sig>
  <id>346780</id>
  <edit-version>1</edit-version>
  <pattern-sets>
    <pattern-set>
      <port>TCP/444-9999</port>
      <protocol>HTTP</protocol>
      <stcpattern>
        axkeiepoep
      </stcpattern>
      <mindata>65534</mindata>
      <ordered>>false</ordered>
      <ctspattern>[a-z][A-Z][0-9]*----[0-9]*</ctspattern>
    </pattern-set>
  </pattern-sets>
</app-sig>

```

```

</pattern-set>
</pattern-sets>
<domain-id>3</domain-id>
<description>
Automated user - custom signature creation with basic type
</description>
<disable-state>>false</disable-state>
<name>custBasicAppSig1</name>
<app-id-version>ALL</app-id-version>
<device-compatibility>X46_AND_OLDER</device-compatibility>
<app-sig-tags>
  <idp-common-value>
    <name>Category</name>
    <value>Remote-Access</value>
  </idp-common-value>
  <idp-common-value>
    <name>Subcategory</name>
    <value>Authentication</value>
  </idp-common-value>
  <idp-common-value>
    <name>Characteristic</name>
    <value />
  </idp-common-value>
  <idp-common-value>
    <name>Risk</name>
    <value>5</value>
  </idp-common-value>
</app-sig-tags>
<definition-type>CUSTOM</definition-type>
<category>Remote-Access</category>
<chainorder>>false</chainorder>
<domain-name>Global</domain-name>
<application-name>custBasicAppSig1</application-name>
<type>protocol</type>
</app-sig>

```

## DELETE

This request is to delete the application signature.

URI	api/juniper/sd/app-sig-management/app-sigs/<app-sig id>
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.app-sig-management.app-sig+json;version=1;charset=UTF-8 application/vnd.juniper.sd.app-sig-management.app-sig+xml;version=1;charset=UTF-8
Consumes	None
Produces	Deletes the application signature.

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)



## CHAPTER 5

# IPS Management RESTful Web Services

- [IPS Management RESTful Web Services on page 41](#)

## IPS Management RESTful Web Services

---

The following operations can be performed using the Security Director IPS Management RESTful Web Services.

### GET

This request is used to get all IPS signature sets configured in Security Director.

URI	/api/juniper/sd/ips-management/ips-sig-sets
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.ips-management.ips-sig-sets+xml;q="0.01";version="1" application/vnd.juniper.sd.ips-management.ips-sig-sets+json;q="0.01";version="1"
Consumes	None
Produces	Collection of IPS signature sets

### Sample IPS Management Input and Output to Get All IPS Signature Sets

URI: /api/juniper/sd/ips-management/ips-sig-sets

This request is used to get all IPS signature sets.

#### Sample XML Output

```
<ips-sig-sets total="9" uri="/api/juniper/sd/ips-management/ips-sig-sets">
  <ips-sig-set href="/api/juniper/sd/ips-management/ips-sig-sets/232479"
uri="/api/juniper/sd/ips-management/ips-sig-sets/232479">
    <name>Web_Server (Predefined) (29)</name>
    <description>This template policy is designed to protect commonly used HTTP servers
from remote attacks.</description>
    <definition-type>PREDEFINED</definition-type>
    <id>232479</id>
  </ips-sig-set>
  <ips-sig-set href="/api/juniper/sd/ips-management/ips-sig-sets/232487"
uri="/api/juniper/sd/ips-management/ips-sig-sets/232487">
```

```
<name>DMZ_Services (Predefined) (40)</name>
<description>This template policy is designed to be used to protect a typical DMZ
environment.</description>
<definition-type>PREDEFINED</definition-type>
<id>232487</id>
</ips-sig-set>
<ips-sig-set href="/api/juniper/sd/ips-management/ips-sig-sets/232495"
uri="/api/juniper/sd/ips-management/ips-sig-sets/232495">
  <name>DNS_Service (Predefined) (11)</name>
  <description>This template policy is designed to protect DNS services. Use this template
as a starting point to customize your desired level of protection.</description>
  <definition-type>PREDEFINED</definition-type>
  <id>232495</id>
  </ips-sig-set>
</ips-sig-sets>
```

#### Sample IPS Management Input and Output to Get IPS Signature Set by ID

URI: /api/juniper/sd/ips-management/ips-sig-sets/232479

This request is used to get IPS signature set by its ID.

#### Sample XML Output

```
<ips-sig-set uri="/api/juniper/sd/ips-management/ips-sig-sets/232479">
  <name>Web_Server (Predefined)</name>
  <description>This template policy is designed to protect commonly used HTTP servers
from remote attacks.</description>
  <edit-version>1</edit-version>
  <definition-type>PREDEFINED</definition-type>
  <created-time>2013-04-24T01:47:24Z</created-time>
  <last-modified-time>2013-04-24T01:47:49Z</last-modified-time>
  <id>232479</id>
  <policy-priority>LOW</policy-priority>
  <priority>2</priority>
  <type>SIGNATURESET</type>
  <signature-sets/>
  <precedence>99</precedence>
  <policy-state>FINAL</policy-state>
</ips-sig-set>
```

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)



## CHAPTER 6

# Variables Management RESTful Web Services

- [Variables Management RESTful Web Services on page 43](#)

## Variables Management RESTful Web Services

---

The following operations can be performed using the Security Director Variables Management RESTful Web Services.

### GET

This request is used to collect all the variables configured in Security Director.

URI	/api/juniper/sd/variable-management/variable-definitions
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.variable-management.variable-definitions+xml;q="0.01";version="1" application/vnd.juniper.sd.variable-management.variable-definitions+json;q="0.01";version="1"
Consumes	None
Produces	Collection of variable definitions

### Sample Variable Management Input and Output to Get All the Variables

URI: /api/juniper/sd/variable-management/variable-definitions

#### Sample XML Output

```
<variable-definitions uri="/api/juniper/sd/variable-management/variable-definitions"
total="2">
  <variable-definition
uri="/api/juniper/sd/variable-management/variable-definitions/33467" href=
"/api/juniper/sd/variable-management/variable-definitions/33467" >
    <name>testVar</name>
    <type>ADDRESS</type>
    <description>test variable </description>
    <domain-name>Global</domain-name>
    <domain-id>2</domain-id>
    <id>33467</id>
```

```

</variable-definition>
<variable-definition
uri="/api/juniper/sd/variable-management/variable-definitions/33470" href=
"/api/juniper/sd/variable-management/variable-definitions/33470" >
<name>testzone</name>
<type>ZONE</type>
<description>test zone variable </description>
<domain-name>Global</domain-name>
<domain-id>2</domain-id>
<id>33470</id>
</variable-definition>
</variable-definitions>

```

### Sample Variable Management input and Output to Get Variable by ID

URI: /api/juniper/sd/variable-management/variable-definitions/655842

Sample XML output to  
get polymorphic  
address by ID

```

<variable-definition
uri="/api/juniper/sd/variable-management/variable-definitions/33467">
<variable-values-list>
<variable-values>
<id>33469</id>
<device>
<moid>
net.juniper.jnap.sm.om.jpaa.SecurityDeviceEntity:32768
</moid>
<name>SRX-119-7</name>
</device>
<variable-value-detail href= "/api/juniper/sd/address-management/addresses/33466"
>
<variable-value>net.juniper.jnap.sm.om.jpaa.AddressEntity:33466</variable-value>
<name>addr1</name>
</variable-value-detail>
<context>DEVICE</context>
</variable-values>
</variable-values-list>
<default-value-detail href= "/api/juniper/sd/address-management/addresses/33399"
>
<default-value>net.juniper.jnap.sm.om.jpaa.AddressEntity:33399</default-value>
</default-value-detail>
<name>testVar</name>
<last-modified-time>2014-04-12T06:23:17Z</last-modified-time>
<created-time>2014-04-12T06:23:17Z</created-time>
<created-by-user-name>super</created-by-user-name>
<definition-type>CUSTOM</definition-type>
<type>ADDRESS</type>
<context>DEVICE</context>
<edit-version>0</edit-version>
<description>test variable </description>
<domain-name>Global</domain-name>
<domain-id>2</domain-id>
<default-name>Any</default-name>
<address-id>33468</address-id>
<id>33467</id>
</variable-definition>

```

Sample XML output to  
get polymorphic zone  
by ID

```
<variable-definition
uri="/api/juniper/sd/variable-management/variable-definitions/33470">
<variable-values-list>
<variable-values>
<id>33471</id>
<device>
<moid>
net.juniper.jnap.sm.om.jpa.SecurityDeviceEntity:32768
</moid>
<name>SRX-119-7</name>
</device>
<variable-value-detail>
<variable-value>zone1</variable-value>
<name>zone1</name>
</variable-value-detail>
<context>DEVICE</context>
</variable-values>
</variable-values-list>
<default-value-detail>
<default-value>trust</default-value>
</default-value-detail>
<name>testzone</name>
<last-modified-time>2014-04-12T06:23:52Z</last-modified-time>
<created-time>2014-04-12T06:23:52Z</created-time>
<created-by-user-name>super</created-by-user-name>
<definition-type>CUSTOM</definition-type>
<type>ZONE</type>
<context>DEVICE</context>
<edit-version>0</edit-version>
<description>test zone variable </description>
<domain-name>Global</domain-name>
<domain-id>2</domain-id>
<default-name>trust</default-name>
<id>33470</id>
</variable-definition>
```

#### Sample Variable Management Input and Output with Pagination

URI	Description
/api/juniper/sd/variable-management/variable-definitions?paging=(limit eq 10)	The first ten variable definitions in the first page are listed.
/api/juniper/sd/variable-management/variable-definitions?paging=(start eq 5, limit eq 10)	Starting from fifth record next 10 records are fetched

#### Sample Variable Management Input and Output with Filtering

URI: /api/juniper/sd/variable-management/variable-definitions?filter=(global eq 'var')

All variable names matching with *var* are filtered.

Sample XML Output

```
<variable-definitions total="2"
uri="/api/juniper/sd/variable-management/variable-definitions">
<variable-definition
```

```

href="/api/juniper/sd/variable-management/variable-definitions/655842"
uri="/api/juniper/sd/variable-management/variable-definitions/655842">
  <name>varzone</name>
  <type>ZONE</type>
  <description>varzone desc modified</description>
  <id>655842</id>
</variable-definition>
<variable-definition
href="/api/juniper/sd/variable-management/variable-definitions/655846"
uri="/api/juniper/sd/variable-management/variable-definitions/655846">
  <name>varaddress</name>
  <type>ADDRESS</type>
  <description>varadd desc modified</description>
  <id>655846</id>
</variable-definition>
</variable-definitions>

```

### Sample Variable Management Input and Output with Sorting

URI	Description
/api/juniper/sd/variable-management/variable-definitions?sortby=(name(ascending))	All variable definition names are sorted in an ascending order.
/api/juniper/sd/variable-management/variable-definitions?sortby=(name(descending))	All variable definition names are sorted in a descending order.

## POST

This request is used to create a variable.

URI	/api/juniper/sd/variable-management/variable-definitions
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.variable-management.variable-definition+xml;version=1; charset=UTF-8 application/vnd.juniper.sd.variable-management.variable-definition+json;version=1; charset=UTF-8
Consumes	None
Produces	Creates a new variable definition

To create a new variable definition, send the new variable information in the Body window, as shown in the following example. This example shows creation of polymorphic address.

#### Sample XML Input

```

<variable-definition>
  <variable-values-list>
    <variable-values>
      <device>
        <moid>net.juniper.jmp.jp LogicalDevice:327752</moid>
        <name>sd-srx240-2</name>
      </device>
    </variable-values>
  </variable-values-list>
</variable-definition>

```

```

<variable-value-detail>
  <variable-value>459012</variable-value>
  <name>User_AD4</name>
</variable-value-detail>
<context>DEVICE</context>
</variable-values>
<variable-values>
  <device>
    <moid>net.juniper.jmp.jp LogicalDevice:327748</moid>
    <name>sd-srx240-1</name>
  </device>
  <variable-value-detail>
    <variable-value>459011</variable-value>
    <name>User_AD3</name>
  </variable-value-detail>
  <context>DEVICE</context>
</variable-values>
</variable-values-list>
<default-value-detail>
  <default-value>1016194</default-value>
</default-value-detail>
<name>var_add1</name>
<created-by-user-name>super</created-by-user-name>
<definition-type>CUSTOM</definition-type>
<type>ADDRESS</type>
<context>DEVICE</context>
<edit-version>1</edit-version>
<description>variable address created using REST</description>
<default-name>User_AD1</default-name>
</variable-definition>

```

The following example shows creation of polymorphic zone:

#### Sample XML Input

```

<variable-definition>
  <name>var_zone1</name>
  <created-by-user-name>super</created-by-user-name>
  <definition-type>CUSTOM</definition-type>
  <type>ZONE</type>
  <default-value />
  <context>DEVICE</context>
  <edit-version>0</edit-version>
  <description>variable zone created using REST</description>
  <default-name>trust</default-name>
  <default-value-detail>
    <default-value> trust </default-value>
  </default-value-detail>
  <variable-values-list>
    <variable-values>
      <id />
    </variable-values>
  </variable-values-list>
  <device>
    <moid>net.juniper.jmp.jp LogicalDevice:327748</moid>
    <name>sd-srx650-4</name>
  </device>
  <variable-value-detail>
    <variable-value> junos-host </variable-value>
    <name>junos-host</name>
  </variable-value-detail>

```

```

    </variable-value-detail>
    <context>DEVICE</context>
  </variable-values>
</variable-values-list>
</variable-definition>

```

## PUT

This request is used to modify a variable.

URI	/api/juniper/sd/variable-management/variable-definitions/{variable-id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.variable-management.variable-definition+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.variable-management.variable-definition+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies a variable definition

To modify a variable definition, send the modify information in the Body window as shown in the following example.

### Sample XML Input

```

<variable-definition>
  <variable-values-list>
    <variable-values>
      <id>1016236</id>
      <device>
        <moid>net.juniper.jmp.jpa.LogicalDevice:327752</moid>
        <name>sd-srx240-2</name>
      </device>
      <variable-value-detail
href="/api/juniper/sd/address-management/addresses/459012">
        <variable-value>net.juniper.jnap.sm.om.jpa.AddressEntity:459012</variable-value>

        <name>User_AD4</name>
      </variable-value-detail>
    </variable-values>
  </variable-values-list>
  <default-value-detail
href="/api/juniper/sd/address-management/addresses/1016194">
    <default-value>net.juniper.jnap.sm.om.jpa.AddressEntity:1016194</default-value>
  </default-value-detail>
  <name>var_add1</name>
  <last-modified-time>2013-04-25T00:02:51+05:30</last-modified-time>
  <created-time>2013-04-25T00:02:51+05:30</created-time>
  <created-by-user-name>super</created-by-user-name>
  <definition-type>CUSTOM</definition-type>
  <type>ADDRESS</type>
  <context>DEVICE</context>
  <edit-version>0</edit-version>

```

```

<description>variable address created using REST</description>
<default-name>User_AD1</default-name>
<id>1016234</id>
</variable-definition>

```

## DELETE

This request is used to delete a variable.

URI	/api/juniper/sd/variable-management/variable-definitions/{variable-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.variable-management.variable-definition+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.variable-management.variable-definition+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes a variable definition

## PATCH

This request is used to patch or to make partial updates to the variable definition.

URI	/api/juniper/sd/variable-management/variable-definitions/{variable-id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.variable-management.variable-definition_patch+xml;version=1;charset=UTF-8
Consumes	None
Produces	Patches a variable definition

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)





CHAPTER 7

# Scheduler Management RESTful Web Services

- Scheduler Management RESTful Web Services on page 51

## Scheduler Management RESTful Web Services

---

The following operations can be performed using the Security Director Scheduler Management RESTful Web Services.

### GET

This request is used to list all the available schedulers.

URI	/api/juniper/sd/scheduler-management/schedulers/
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.scheduler-management.scheduler+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.scheduler-management.scheduler+json;version=1;charset=UTF-8
Consumes	None
Produces	Lists schedulers

Sample XML Output	<schedulers total="4" uri="/api/juniper/sd/scheduler-management/schedulers/"> <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426244" uri="/api/juniper/sd/scheduler-management/schedulers/426244"> <name>scheduler_Empty</name> <description>scheduler_Empty </description> <id>426244</id> </scheduler> <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426245" uri="/api/juniper/sd/scheduler-management/schedulers/426245"> <name>scheduler_1</name> <description>scheduler_1</description> <id>426245</id> </scheduler> <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426249" uri="/api/juniper/sd/scheduler-management/schedulers/426249">
-------------------	--

```

<name>scheduler_2</name>
<description>scheduler_2</description>
<id>426249</id>
</scheduler>
<scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426250"
uri="/api/juniper/sd/scheduler-management/schedulers/426250">
  <name>scheduler_3</name>
  <description>scheduler_2</description>
  <id>426250</id>
</scheduler>
</schedulers>

```

### Sample Scheduler Management Input and Output with Pagination:

URI: /api/juniper/sd/scheduler-management/schedulers?paging=(limit eq 3)	The first 3 schedulers in the first page are listed.
--	--

URI: /api/juniper/sd/scheduler-management/schedulers?paging=(start eq 1, limit eq 2)	Start with record number 1 next 2 records are fetched
--	---

### Sample Scheduler Management Input and Output with Filtering

You can search for schedulers with global key words and with names as well.

URI: /api/juniper/sd/scheduler-management/schedulers?filter=(global eq 'scheduler\*')

All schedulers matching with *scheduler* name are filtered.

#### Sample XML Output

```

<schedulers total="4" uri="/api/juniper/sd/scheduler-management/schedulers/">
  <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426244"
uri="/api/juniper/sd/scheduler-management/schedulers/426244">
    <name>scheduler_Empty</name>
    <description>scheduler_Empty </description>
    <id>426244</id>
  </scheduler>
  <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426245"
uri="/api/juniper/sd/scheduler-management/schedulers/426245">
    <name>scheduler_1</name>
    <description>scheduler_1</description>
    <id>426245</id>
  </scheduler>
  <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426249"
uri="/api/juniper/sd/scheduler-management/schedulers/426249">
    <name>scheduler_2</name>
    <description>scheduler_2</description>
    <id>426249</id>
  </scheduler>
  <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426250"
uri="/api/juniper/sd/scheduler-management/schedulers/426250">
    <name>scheduler_3</name>
    <description>scheduler_2</description>
    <id>426250</id>
  </scheduler>
</schedulers>

```

URI: /api/juniper/sd/scheduler-management/schedulers?filter=(name eq 'scheduler\_2')

Scheduler with name *scheduler\_2* is only filtered.

**Sample XML Output**

```
<schedulers total="4" uri="/api/juniper/sd/scheduler-management/schedulers/">
  <scheduler href= "/api/juniper/sd/scheduler-management/schedulers/426249"
uri="/api/juniper/sd/scheduler-management/schedulers/426249">
    <name>scheduler_2</name>
    <description>scheduler_2</description>
    <id>426249</id>
  </scheduler>
</schedulers>
```

### Sample Scheduler Management Input and Output with Sorting

URI	Description
/api/juniper/sd/scheduler-management/schedulers?sortby=(name(ascending))	Scheduler names are listed in an ascending order.
/api/juniper/sd/scheduler-management/schedulers?sortby=(name(descending))	Scheduler names are listed in descending order.

## POST

This request is used to create a new scheduler.

URI	/api/juniper/sd/scheduler-management/schedulers/
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.scheduler-management.scheduler+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.scheduler-management.scheduler+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new scheduler

**Sample XML Input**

```
<scheduler>
  <name>scheduler_1</name>
  <description>scheduler_1</description>
  <start-date1>2013-04-10.23:23</start-date1>
  <stop-date1>2013-04-12.12:12</stop-date1>
  <start-date2>2013-04-16.03:23</start-date2>
  <stop-date2>2013-04-18.04:12</stop-date2>
  <schedules>
    <schedule>
      <day>MONDAY</day>
      <start-time1 />
      <stop-time1 />
      <start-time2 />
      <stop-time2 />
      <exclude>true</exclude>
```

```

    <all-day>false</all-day>
  </schedule>
  <schedule>
    <day>TUESDAY</day>
    <start-time1 />
    <stop-time1 />
    <start-time2 />
    <stop-time2 />
    <exclude>false</exclude>
    <all-day>true</all-day>
  </schedule>
  <schedule>
    <day>WEDNESDAY</day>
    <start-time1>12:12:12</start-time1>
    <stop-time1>13:13:13</stop-time1>
    <start-time2>08:12:02</start-time2>
    <stop-time2>12:12:12</stop-time2>
    <exclude>false</exclude>
    <all-day>false</all-day>
  </schedule>
</schedules>
<definition-type>CUSTOM</definition-type>
</scheduler>

```

### Modify a Scheduler

This request is used to modify an existing scheduler.

URI: /api/juniper/sd/scheduler-management/schedulers/426250

#### Sample XML Input

```

<scheduler uri="/api/juniper/sd/scheduler-management/schedulers/426250">
  <name>scheduler_3</name>
  <description>scheduler_2</description>
  <start-date1>2013-05-12.03:15</start-date1>
  <stop-date1>2013-05-14.04:10</stop-date1>
  <schedules
    uri="/api/juniper/sd/scheduler-management/schedulers/426250/schedules">
    <schedule>
      <day>DAILY</day>
      <start-time1>01:01:01</start-time1>
      <stop-time1>02:02:02</stop-time1>
      <start-time2> </start-time2>
      <stop-time2> </stop-time2>
      <exclude>false</exclude>
      <all-day>false</all-day>
    </schedule>
    <schedule>
      <day>MONDAY</day>
      <start-time1> </start-time1>
      <stop-time1> </stop-time1>
      <start-time2> </start-time2>
      <stop-time2> </stop-time2>
      <exclude>false</exclude>
      <all-day>true</all-day>
    </schedule>
  </schedules>
</scheduler>

```

```

<day>TUESDAY</day>
<start-time1> </start-time1>
<stop-time1> </stop-time1>
<start-time2> </start-time2>
<stop-time2> </stop-time2>
<exclude>true</exclude>
<all-day>>false</all-day>
</schedule>
</schedules>
<edit-version>1</edit-version>
<definition-type>CUSTOM</definition-type>
<id>426250</id>
</scheduler>

```

## DELETE

This request is used to delete a scheduler.

URI	/api/juniper/sd/scheduler-management/schedulers/426250
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.scheduler-management.scheduler+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.scheduler-management.scheduler+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes a scheduler

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)



CHAPTER 8

# UTM Management RESTful Web Services

- [UTM Policy Management RESTful Web Services on page 57](#)
- [Antispam Profile Management RESTful Web Services on page 62](#)
- [Antivirus Profile Management RESTful Web Services on page 64](#)
- [Content Filtering Profile Management RESTful Web Services on page 68](#)
- [Web Filtering Profile Management RESTful Web Services on page 73](#)
- [URL Pattern Management RESTful Web Services on page 78](#)
- [URL Category Management RESTful Web Services on page 81](#)
- [Device Profile Management RESTful Web Services on page 85](#)

## UTM Policy Management RESTful Web Services

The following operations can be performed using the Security Director UTM Policy Management RESTful Web Services.

### GET

This request is used to list all the available UTM Policies.

URI	api/juniper/sd/utm-management/utm-policies
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.utm-management.utm-policy-refs+xml;version=1 application/vnd.juniper.sd.utm-management.utm-policy-refs+json;version=1
Consumes	None
Produces	Collection of UTM policies.

**Sample XML Output**

```
<utm-policies uri="/api/juniper/sd/utm-management/utm-policies" total="9">
  <utm-policy href="/api/juniper/sd/utm-management/utm-policies/98542"
uri="/api/juniper/sd/utm-management/utm-policies/98542">
    <name>av-policy</name>
    <id>98542</id>
    <domain-name>SYSTEM</domain-name>
    <domain-id>1</domain-id>
```

```
<definition-type>PREDEFINED</definition-type>
</utm-policy>
```

### Sample Input and Output to Get UTM Policies by ID

URI: `api/juniper/sd/utm-management/utm-policies/{id}`

#### Sample XML Output

```
<utm-policy uri="/api/juniper/sd/utm-management/utm-policies/99678">
  <name>HR-Policy</name>
  <domain-name>Global</domain-name>
  <domain-id>2</domain-id>
  <id>99678</id>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <session-over-limit-action>NONE</session-over-limit-action>
  <anti-spam-profile href=
"/api/juniper/sd/utm-management/anti-spam-profiles/98315" >
    <id>98315</id>
    <domain-id>1</domain-id>
    <name>as-defaults</name>
  </anti-spam-profile>
  <content-filtering-profiles>
    <smtp-profile/>
    <pop3-profile/>
    <imap-profile/>
    <ftp-upload-profile/>
    <ftp-download-profile/>
    <http-profile/>
    <default-profile/>
  </content-filtering-profiles>
  <web-filtering-profile href=
"/api/juniper/sd/utm-management/web-filtering-profiles/99672" >
    <id>99672</id>
    <domain-id>2</domain-id>
    <name>custom-websense</name>
  </web-filtering-profile>
  <anti-virus-profiles>
    <smtp-profile/>
    <pop3-profile href= "/api/juniper/sd/utm-management/anti-virus-profiles/99665"
  >
    <id>99665</id>
    <domain-id>2</domain-id>
    <name>Custom-juniper-express-engine</name>
    </pop3-profile>
    <imap-profile/>
    <ftp-upload-profile/>
    <ftp-download-profile/>
    <http-profile/>
    <default-profile/>
  </anti-virus-profiles>
  <sessions-per-client>0</sessions-per-client>
</utm-policy>
```



## POST

This request is used to create a new UTM policy.

URI	api/juniper/sd/utm-management/utm-policies
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.utm-policy+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.utm-policy+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new UTM policy.

### Sample XML Input

```
<utm-policy >
  <name>HR-Policy</name>
  <description>This is created using REST</description>
  <session-over-limit-action>BLOCK</session-over-limit-action>
  <anti-spam-profile >
    <id>128564</id>
    <name>custom-sb2</name>
  </anti-spam-profile>
  <content-filtering-profiles>
    <smtp-profile/>
    <pop3-profile/>
    <imap-profile/>
    <ftp-upload-profile/>
    <ftp-download-profile>
      <id>121502</id>
      <name>Test1</name>
    </ftp-download-profile>
    <http-profile>
      <id>121501</id>
      <name>Test</name>
    </http-profile>
    <default-profile/>
  </content-filtering-profiles>
  <web-filtering-profile>
    <id>128588</id>
    <name>custom-juniper-enhanced</name>
  </web-filtering-profile>
  <anti-virus-profiles>
    <smtp-profile>
      <id>128579</id>
      <name>Custom-juniper-express-engine</name>
    </smtp-profile>
    <pop3-profile>
      <id>128579</id>
      <name>Custom-juniper-express-engine</name>
    </pop3-profile>
    <imap-profile>
      <id>128579</id>
```

```

    <name>Custom-juniper-express-engine</name>
  </imap-profile>
  <ftp-upload-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </ftp-upload-profile>
  <ftp-download-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </ftp-download-profile>
  <http-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </http-profile>
  <default-profile/>
</anti-virus-profiles>
<sessions-per-client>123</sessions-per-client>
</utm-policy>

```

## PUT

This request is used to modify UTM policy.

URI	api/juniper/sd/utm-management/utm-policies/{id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.utm-policy+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.utm-policy+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the UTM policy.

### Sample XML Input

```

<utm-policy>
  <name>HR-Policy</name>
  <description>This is created using REST</description>
  <id>128831</id>
  <edit-version>1</edit-version>
  <session-over-limit-action>BLOCK</session-over-limit-action>
  <anti-spam-profile href=
"/api/juniper/sd/utm-management/anti-spam-profiles/128564" >
    <id>128564</id>
    <name>custom-sb2</name>
  </anti-spam-profile>
  <content-filtering-profiles>
    <smtp-profile/>
    <pop3-profile/>
    <imap-profile/>
    <ftp-upload-profile/>
    <ftp-download-profile>
      <id>121502</id>
      <name>Test1</name>
    </ftp-download-profile>
  </content-filtering-profiles>
</utm-policy>

```

```

</ftp-download-profile>
<http-profile>
  <id>121501</id>
  <name>Test</name>
</http-profile>
<default-profile/>
</content-filtering-profiles>
<web-filtering-profile>
  <id>128588</id>
  <name>custom-juniper-enhanced</name>
</web-filtering-profile>
<anti-virus-profiles>
  <smtp-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </smtp-profile>
  <pop3-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </pop3-profile>
  <imap-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </imap-profile>
  <ftp-upload-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </ftp-upload-profile>
  <ftp-download-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </ftp-download-profile>
  <http-profile>
    <id>128579</id>
    <name>Custom-juniper-express-engine</name>
  </http-profile>
  <default-profile/>
</anti-virus-profiles>
<sessions-per-client>123</sessions-per-client>
</utm-policy>

```

## DELETE

This request is used to delete UTM policy.

URI	api/juniper/sd/utm-management/utm-policies/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.utm-policy+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.utm-policy+xml;version=1;charset=UTF-8
Consumes	None

Produces

Deletes UTM policy.

**Related  
Documentation**

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

## Antispam Profile Management RESTful Web Services

The following operations can be performed using the Security Director Antispam RESTful Web Services.

### GET

This request is used to list all the available antispam objects.

URI	api/juniper/sd/utm-management/anti-spam-profiles
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.utm-management.anti-spam-profile-refs+xml;version=1;q=0.01 application/vnd.juniper.sd.utm-management.anti-spam-profile-refs+json;version=1;q=0.01
Consumes	None
Produces	Collection of antispam objects.

**Sample XML Output**

```
<anti-spam-profiles uri="/api/juniper/sd/utm-management/anti-spam-profiles/"
total="4">
  <anti-spam-profile href=
"/api/juniper/sd/utm-management/anti-spam-profiles/98315"
uri="/api/juniper/sd/utm-management/anti-spam-profiles/98315">
    <name>as-defaults</name>
    <id>98315</id>
    <domain-name>SYSTEM</domain-name>
    <domain-id>1</domain-id>
    <definition-type>PREDEFINED</definition-type>
  </anti-spam-profile>
```

**Sample Input and Output to Get the Antispam Profile by ID**

URI: api/juniper/sd/utm-management/anti-spam-profile/{id}

**Sample XML Output**

```
<anti-spam-profile uri="/api/juniper/sd/utm-management/anti-spam-profiles/99555">

  <name>EMail-Policy</name>
  <id>99555</id>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <default-action>TAG_HEADER</default-action>
  <tag-string>This is blocked by AntiSpam</tag-string>
  <default-sbl-server>true</default-sbl-server>
  <created-by-user-name>super</created-by-user-name>
```

```

<last-modified-by-user-name>super</last-modified-by-user-name>
<domain-name>Domain-1</domain-name>
<domain-id>4375</domain-id>
</anti-spam-profile>

```

## POST

This request is used to create a new antis spam profile.

URI	api/juniper/sd/utm-management/anti-spam-profiles
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.anti-spam-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.anti-spam-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new antis spam profile.

### Sample XML Input

```

<anti-spam-profile>
  <name>AntiSpam-Profile-1</name>
  <default-action>TAG_SUBJECT</default-action>
  <default-sbl-server>true</default-sbl-server>
</anti-spam-profile>

```

## PUT

This request is used to modify an antis spam profile.

URI	api/juniper/sd/utm-management/anti-spam-profiles/{id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.anti-spam-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.anti-spam-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies an antis spam profile.

### Sample XML Input

```

<anti-spam-profile>
  <name>AntiSpam-Profile-1</name>
  <id>128818</id>
  <edit-version>2</edit-version>
  <default-action>TAG_SUBJECT</default-action>
  <default-sbl-server>false</default-sbl-server>
</anti-spam-profile>

```

## DELETE

This request is used to delete an antispam profile.

URI	api/juniper/sd/utm-management/anti-spam-profiles/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.anti-spam-profile+xml;version="1" application/vnd.juniper.sd.utm-management.anti-spam-profile+json;version="1"
Consumes	None
Produces	Deletes an antispam profile.

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)

## Antivirus Profile Management RESTful Web Services

The following operations can be performed using the Security Director Antivirus RESTful Web Services.

### GET

This request is used to list all the available antivirus objects.

URI	api/juniper/sd/utm-management/anti-virus-profiles
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.utm-management.anti-virus-profile-refs+xml;version=1;q=0.01 application/vnd.juniper.sd.utm-management.anti-virus-profile-refs+json;version=1;q=0.01
Consumes	None
Produces	Collection of antivirus objects.

#### Sample XML Output

```
<anti-virus-profiles uri="/api/juniper/sd/utm-management/anti-virus-profiles"
total="6">
  <anti-virus-profile href= "/api/juniper/sd/utm-management/anti-virus-profiles/98316"
uri="/api/juniper/sd/utm-management/anti-virus-profiles/98316">
    <name>av-defaults</name>
    <id>98316</id>
    <domain-name>SYSTEM</domain-name>
    <domain-id>1</domain-id>
    <definition-type>PREDEFINED</definition-type>
  </anti-virus-profile>
```

```

<anti-virus-profile href="/api/juniper/sd/utm-management/anti-virus-profiles/98317"
uri="/api/juniper/sd/utm-management/anti-virus-profiles/98317">
  <name>sophos-av-defaults</name>
  <id>98317</id>
  <domain-name>SYSTEM</domain-name>
  <domain-id>1</domain-id>
  <definition-type>PREDEFINED</definition-type>
</anti-virus-profile>

```

### Sample Input and Output to Get Antivirus Objects by ID

URI: `api/juniper/sd/utm-management/anti-virus-profiles/{id}`

#### Sample XML Output

```

<anti-virus-profile uri="/api/juniper/sd/utm-management/anti-virus-profiles/99559">

  <name>AV-sophos</name>
  <domain-name>Domain-1</domain-name>
  <domain-id>4375</domain-id>
  <id>99559</id>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <trickling-timeout>100</trickling-timeout>
  <virus-detection-notification-options>
    <custom-notification-message>Message Subject line</custom-notification-message>

    <notification-type>MESSAGE</notification-type>
    <custom-notification-subject>test123</custom-notification-subject>
    <notify-mail-sender>true</notify-mail-sender>
  </virus-detection-notification-options>
  <fallback-block-notification-options>
    <fallback-block-notification-option>
      <custom-notification-message>test123</custom-notification-message>
      <notification-type>PROTOCOL</notification-type>
      <custom-notification-subject>abc12345</custom-notification-subject>
      <notify-mail-sender>true</notify-mail-sender>
    </fallback-block-notification-option>
    <allow-email>false</allow-email>
    <display-host-name>false</display-host-name>
  </fallback-block-notification-options>
  <fallback-non-block-notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <custom-notification-subject>Message Subject line</custom-notification-subject>
    <notify-mail-sender>true</notify-mail-sender>
  </fallback-non-block-notification-options>
  <scan-options>
    <content-size-limit>10000</content-size-limit>
  </scan-options>
  <fallback-options>
    <fallback-option>
      <engine-error>BLOCK</engine-error>
      <default-action>BLOCK</default-action>
    </fallback-option>
    <content-size>BLOCK</content-size>
  </fallback-options>
  <profile-type>SOPHOS</profile-type>
  <created-by-user-name>super</created-by-user-name>

```

```
<last-modified-by-user-name>super</last-modified-by-user-name>
</anti-virus-profile>
```

## POST

This request is used to create a new antivirus profile.

URI	api/juniper/sd/utm-management/anti-virus-profiles
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.anti-virus-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.anti-virus-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new antivirus profile.

### sample XML Input

```
<anti-virus-profile>
  <name>AntiVirus-Profile-1</name>
  <description>This profile is created using REST</description>
  <trickling-timeout>123</trickling-timeout>
  <virus-detection-notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <notification-type>PROTOCOL</notification-type>
    <custom-notification-subject>This is blocked</custom-notification-subject>
    <notify-mail-sender>true</notify-mail-sender>
  </virus-detection-notification-options>
  <fallback-block-notification-options>
    <fallback-block-notification-option>
      <custom-notification-message>This is blocked</custom-notification-message>
      <notification-type>PROTOCOL</notification-type>
      <custom-notification-subject>This is blocked</custom-notification-subject>
      <notify-mail-sender>true</notify-mail-sender>
    </fallback-block-notification-option>
    <allow-email>true</allow-email>
    <display-host-name>true</display-host-name>
    <administrator-email-address>admin@example.com</administrator-email-address>
  </fallback-block-notification-options>
  <fallback-non-block-notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <custom-notification-subject>This is blocked</custom-notification-subject>
    <notify-mail-sender>true</notify-mail-sender>
  </fallback-non-block-notification-options>
  <scan-options>
    <content-size-limit>123</content-size-limit>
    <scan-file-extension>zip</scan-file-extension>
    <scan-file-extension>jpg</scan-file-extension>
    <scan-file-extension>rar</scan-file-extension>
  </scan-options>
  <fallback-options>
    <fallback-option>
```



```

<engine-error>LOG_AND_PERMIT</engine-error>
<default-action>LOG_AND_PERMIT</default-action>
</fallback-option>
<decompress-layer>LOG_AND_PERMIT</decompress-layer>
<password-file>LOG_AND_PERMIT</password-file>
<content-size>LOG_AND_PERMIT</content-size>
<corrupt-file>LOG_AND_PERMIT</corrupt-file>
</fallback-options>
<profile-type>KASPERSKY</profile-type>
</anti-virus-profile>

```

## PUT

This request is used to modify an antivirus profile.

URI	api/juniper/sd/utm-management/anti-virus-profiles/{id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.anti-virus-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.anti-virus-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies an antivirus profile.

### Sample XML Input

```

<anti-virus-profile>
  <name>AntiVirus-Profile-1</name>
  <description>This profile is created using REST</description>
  <id>128818</id>
  <edit-version>2</edit-version>
  <trickling-timeout>111</trickling-timeout>
  <virus-detection-notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <notification-type>PROTOCOL</notification-type>
    <custom-notification-subject>This is blocked</custom-notification-subject>
    <notify-mail-sender>true</notify-mail-sender>
  </virus-detection-notification-options>
  <fallback-block-notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <notification-type>PROTOCOL</notification-type>
    <custom-notification-subject>This is blocked</custom-notification-subject>
    <notify-mail-sender>true</notify-mail-sender>
  </fallback-block-notification-option>
  <allow-email>true</allow-email>
  <display-host-name>true</display-host-name>
  <administrator-email-address>admin1@example.com</administrator-email-address>

  </fallback-block-notification-options>
  <fallback-non-block-notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <custom-notification-subject>This is blocked</custom-notification-subject>

```

```

<notify-mail-sender>true</notify-mail-sender>
</fallback-non-block-notification-options>
<scan-options>
  <content-size-limit>123</content-size-limit>
  <scan-file-extension>zip</scan-file-extension>
  <scan-file-extension>rar</scan-file-extension>
  <scan-file-extension>jpg</scan-file-extension>
</scan-options>
<fallback-options>
  <fallback-option>
    <engine-error>LOG_AND_PERMIT</engine-error>
    <default-action>LOG_AND_PERMIT</default-action>
  </fallback-option>
  <decompress-layer>LOG_AND_PERMIT</decompress-layer>
  <password-file>LOG_AND_PERMIT</password-file>
  <content-size>LOG_AND_PERMIT</content-size>
  <corrupt-file>LOG_AND_PERMIT</corrupt-file>
</fallback-options>
<profile-type>KASPERSKY</profile-type>
</anti-virus-profile>

```

## DELETE

This request is used to delete an antivirus profile.

URI	api/juniper/sd/utm-management/anti-virus-profiles/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.anti-virus-profile+xml;version="1" application/vnd.juniper.sd.utm-management.anti-virus-profile+json;version="1"
Consumes	None
Produces	Deletes an antivirus profile.

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)

## Content Filtering Profile Management RESTful Web Services

The following operations can be performed using the Security Director Content Filtering Profile Management RESTful Web Services.

## GET

This request is used to list all the available content filtering objects.

URI	/api/juniper/sd/utm-management/content-filtering-profiles
-----	---

HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.utm-management.content-filtering-profile-refs+xml;version=1;q=0.01 application/vnd.juniper.sd.utm-management.content-filtering-profile-refs+json;version=1;q=0.01
Consumes	None
Produces	Collection of content filtering objects.

**Sample XML Output**

```
<content-filtering-profiles
uri="/api/juniper/sd/utm-management/content-filtering-profiles" total="2">
  <content-filtering-profile href=
"/api/juniper/sd/utm-management/content-filtering-profiles/121501"
uri="/api/juniper/sd/utm-management/content-filtering-profiles/121501">
    <name>Test</name>
    <description>Test</description>
    <id>121501</id>
    <domain-name>Global</domain-name>
    <domain-id>2</domain-id>
    <definition-type>CUSTOM</definition-type>
  </content-filtering-profile>
  <content-filtering-profile href=
"/api/juniper/sd/utm-management/content-filtering-profiles/121502"
uri="/api/juniper/sd/utm-management/content-filtering-profiles/121502">
```

**Sample Input and Output to Get Content Filtering Objects by ID**

URI: /api/juniper/sd/utm-management/content-filtering-profiles/{id}

**Sample XML Output**

```
<content-filtering-profile
uri="/api/juniper/sd/utm-management/content-filtering-profiles/99561">
  <name>custom-content-filtering</name>
  <domain-name>Domain-1</domain-name>
  <domain-id>4375</domain-id>
  <id>99561</id>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <permit-command-list>
    <permit-command>pass</permit-command>
    <permit-command>port</permit-command>
    <permit-command>type</permit-command>
    <permit-command>user</permit-command>
  </permit-command-list>
  <block-content-type-list>
    <block-content-type>ACTIVEX</block-content-type>
    <block-content-type>EXE</block-content-type>
    <block-content-type>JAVA_APPLET</block-content-type>
    <block-content-type>HTTP_COOKIE</block-content-type>
    <block-content-type>ZIP</block-content-type>
  </block-content-type-list>
  <block-file-extension-list>
    <block-file-extension>ADE</block-file-extension>
    <block-file-extension>ADP</block-file-extension>
    <block-file-extension>BAS</block-file-extension>
```

```

<block-file-extension>BAT</block-file-extension>
<block-file-extension>CHM</block-file-extension>
<block-file-extension>CMD</block-file-extension>
<block-file-extension>COM</block-file-extension>
<block-file-extension>CPL</block-file-extension>
<block-file-extension>CRT</block-file-extension>
<block-file-extension>DE</block-file-extension>
<block-file-extension>DLL</block-file-extension>
<block-file-extension>DOT</block-file-extension>
<block-file-extension>EXE</block-file-extension>
<block-file-extension>HLP</block-file-extension>
<block-file-extension>HTA</block-file-extension>
<block-file-extension>INF</block-file-extension>
<block-file-extension>INS</block-file-extension>
<block-file-extension>ISP</block-file-extension>
<block-file-extension>JS</block-file-extension>
<block-file-extension>JSE</block-file-extension>
<block-file-extension>LNK</block-file-extension>
<block-file-extension>MDB</block-file-extension>
<block-file-extension>MDE</block-file-extension>
<block-file-extension>MSC</block-file-extension>
<block-file-extension>VBS</block-file-extension>
<block-file-extension>WSC</block-file-extension>
<block-file-extension>WSF</block-file-extension>
<block-file-extension>WSH</block-file-extension>
<block-file-extension>XL</block-file-extension>
</block-file-extension-list>
<notification-options>
  <custom-notification-message>abcd</custom-notification-message>
  <notification-type>PROTOCOL</notification-type>
  <notify-mail-sender>true</notify-mail-sender>
</notification-options>
<block-command-list>
  <block-command>pass</block-command>
  <block-command>port</block-command>
  <block-command>type</block-command>
  <block-command>user</block-command>
</block-command-list>
<block-mime-list>
  <block-mime>image/x-portable-anymap</block-mime>
  <block-mime>video/quicktime</block-mime>
  <block-mime>x-world/x-vrml</block-mime>
</block-mime-list>
<block-mime-exception-list>
  <block-mime-exception>video/quicktime-inappropriate</block-mime-exception>
</block-mime-exception-list>
<created-by-user-name>super</created-by-user-name>
<last-modified-by-user-name>super</last-modified-by-user-name>
</content-filtering-profile>

```

## POST

This request is used to create a new content filtering profile.

URI	/api/juniper/sd/utm-management/content-filtering-profiles
-----	---

HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.content-filtering-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.content-filtering-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new content filtering profile.

**Sample XML Input**

```
<content-filtering-profile>
  <name>Content-Filtering-1</name>
  <description>This Profile is created using REST</description>
  <definition-type>CUSTOM</definition-type>
  <permit-command-list>
    <permit-command>user</permit-command>
    <permit-command>pass</permit-command>
    <permit-command>port</permit-command>
  </permit-command-list>
  <block-content-type-list>
    <block-content-type>ACTIVEX</block-content-type>
    <block-content-type>EXE</block-content-type>
    <block-content-type>HTTP_COOKIE</block-content-type>
    <block-content-type>JAVA_APPLET</block-content-type>
    <block-content-type>ZIP</block-content-type>
  </block-content-type-list>
  <block-file-extension-list>
    <block-file-extension>port/type</block-file-extension>
  </block-file-extension-list>
  <notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <notification-type>PROTOCOL</notification-type>
    <notify-mail-sender>true</notify-mail-sender>
  </notification-options>
  <block-command-list>
    <block-command>set</block-command>
    <block-command>cat</block-command>
    <block-command>exe</block-command>
  </block-command-list>
  <block-mime-list>
    <block-mime>mime1/mime2</block-mime>
    <block-mime>mime3/mime4</block-mime>
  </block-mime-list>
  <block-mime-exception-list>
    <block-mime-exception>get/set</block-mime-exception>
    <block-mime-exception>put/post</block-mime-exception>
  </block-mime-exception-list>
</content-filtering-profile>
```

**PUT**

This request is used to modify the content filtering profile.

URI	/api/juniper/sd/utm-management/content-filtering-profiles/{id}
-----	--

HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.content-filtering-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.content-filtering-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the content filtering profile.

**Sample XML Input**

```

<content-filtering-profile>
  <name>Content-Filtering-1</name>
  <description>This Profile is created using REST</description>
  <id>128819</id>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <permit-command-list>
    <permit-command>user</permit-command>
    <permit-command>pass</permit-command>
    <permit-command>port</permit-command>
  </permit-command-list>
  <block-content-type-list>
    <block-content-type>ACTIVEX</block-content-type>
    <block-content-type>EXE</block-content-type>
    <block-content-type>HTTP_COOKIE</block-content-type>
    <block-content-type>JAVA_APPLET</block-content-type>
    <block-content-type>ZIP</block-content-type>
  </block-content-type-list>
  <block-file-extension-list>
    <block-file-extension>port/type</block-file-extension>
  </block-file-extension-list>
  <notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <notification-type>PROTOCOL</notification-type>
    <notify-mail-sender>true</notify-mail-sender>
  </notification-options>
  <block-command-list>
    <block-command>set</block-command>
    <block-command>cat</block-command>
    <block-command>exe</block-command>
  </block-command-list>
  <block-mime-list>
    <block-mime>asd/sdf</block-mime>
    <block-mime>dfg/fgh</block-mime>
  </block-mime-list>
  <block-mime-exception-list>
    <block-mime-exception>get/set</block-mime-exception>
    <block-mime-exception>put/post</block-mime-exception>
  </block-mime-exception-list>
</content-filtering-profile>

```

## DELETE

This request is used to delete the content filtering profile.

URI	/api/juniper/sd/utm-management/content-filtering-profiles/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.content-filtering-profile+xml;version="1" application/vnd.juniper.sd.utm-management.content-filtering-profile+json;version="1"
Consumes	None
Produces	Deletes the content filtering profile.

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)

## Web Filtering Profile Management RESTful Web Services

The following operations can be performed using the Security Director Web Filtering Management RESTful Web Services.

## GET

This request is used to list all the available web filtering objects.

URI	api/juniper/sd/utm-management/web-filtering-profiles
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.utm-management.web-filtering-profile-refs+xml;version=1;q=0.01 application/vnd.juniper.sd.utm-management.web-filtering-profile-refs+json;version=1;q=0.01
Consumes	None
Produces	Collection of web filtering objects.

### Sample XML Output

```
<web-filtering-profiles uri="/api/juniper/sd/utm-management/web-filtering-profiles"
total="10">
  <web-filtering-profile href=
"/api/juniper/sd/utm-management/web-filtering-profiles/98489"
uri="/api/juniper/sd/utm-management/web-filtering-profiles/98489">
    <name>wf-cpa-default</name>
    <domain-name>SYSTEM</domain-name>
    <domain-id>1</domain-id>
    <id>98489</id>
```

```
<definition-type>PREDEFINED</definition-type>
</web-filtering-profile>
<web-filtering-profile href=
"/api/juniper/sd/utm-management/web-filtering-profiles/98530"
uri="/api/juniper/sd/utm-management/web-filtering-profiles/98530">
```

### Sample Input and Output to Get Web Profiles by ID

URI: `api/juniper/sd/utm-management/web-filtering-profiles`

#### Sample XML Output

```
<web-filtering-profile
uri="/api/juniper/sd/utm-management/web-filtering-profiles/99674">
<name>HR-Filters</name>
<description>
This applies to all HR groups
</description>
<domain-name>Global</domain-name>
<domain-id>2</domain-id>
<id>99674</id>
<edit-version>1</edit-version>
<definition-type>CUSTOM</definition-type>
<safe-search>>false</safe-search>
<custom-block-message>This site is denied</custom-block-message>
<url-category-action-list>
<url-category-action>
<action>LOG_AND_PERMIT</action>
<reputation-action/>
<url-category-list href= "/api/juniper/sd/utm-management/url-category-lists/98379"
>
<id>98379</id>
<domain-id>1</domain-id>
<domain-name>SYSTEM</domain-name>
<name>Enhanced_Vehicles</name>
</url-category-list>
</url-category-action>
<url-category-action>
<action>LOG_AND_PERMIT</action>
<reputation-action/>
<url-category-list href= "/api/juniper/sd/utm-management/url-category-lists/98466"
>
<id>98466</id>
<domain-id>1</domain-id>
<domain-name>SYSTEM</domain-name>
<name>Enhanced_Web_Collaboration</name>
</url-category-list>
</url-category-action>
</url-category-action-list>
<site-reputation-actions>
<moderately-safe>LOG_AND_PERMIT</moderately-safe>
<harmful>BLOCK</harmful>
<suspicious>BLOCK</suspicious>
<very-safe>PERMIT</very-safe>
<fairly-safe>LOG_AND_PERMIT</fairly-safe>
</site-reputation-actions>
<default-action>LOG_AND_PERMIT</default-action>
<fallback-default-action>LOG_AND_PERMIT</fallback-default-action>
```



```

<profile-type>JUNIPER_ENHANCED</profile-type>
<timeout>1200</timeout>
</web-filtering-profile>

```

## POST

This request is used to create a new web filtering profile.

URI	api/juniper/sd/utm-management/web-filtering-profiles
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.web-filtering-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.web-filtering-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new web filtering profile.

### Sample XML Input

```

<web-filtering-profile>
  <name>Web-Policy</name>
  <description>This is created using REST</description>
  <safe-search>true</safe-search>
  <custom-block-message>This is blocked</custom-block-message>
  <quarantine-custom-message>This is blocked</quarantine-custom-message>
  <url-category-action-list>
    <url-category-action>
      <action>BLOCK</action>
      <reputation-action/>
    </url-category-action>
  </url-category-action-list>
  <id>98368</id>
  <name>Enhanced_Abortion</name>
  </url-category-action-list>
  </url-category-action>
  <url-category-action>
    <action>PERMIT</action>
    <reputation-action/>
  </url-category-action-list>
  <id>98427</id>
  <name>Enhanced_Internet_Telephony</name>
  </url-category-action-list>
  </url-category-action>
  <url-category-action>
    <action>QUARANTINE</action>
    <reputation-action/>
  </url-category-action-list>
  <id>98422</id>
  <name>Enhanced_Pay_to_Surf</name>
  </url-category-action-list>
  </url-category-action>
  </url-category-action-list>
  <site-reputation-actions>
    <moderately-safe>PERMIT</moderately-safe>
  </site-reputation-actions>
</web-filtering-profile>

```

```

<harmful>BLOCK</harmful>
<suspicious>LOG_AND_PERMIT</suspicious>
<very-safe>PERMIT</very-safe>
<fairly-safe>LOG_AND_PERMIT</fairly-safe>
</site-reputation-actions>
<default-action>LOG_AND_PERMIT</default-action>
<fallback-default-action>LOG_AND_PERMIT</fallback-default-action>
<profile-type>JUNIPER_ENHANCED</profile-type>
<timeout>15</timeout>
</web-filtering-profile>

```

## PUT

This request is used to modify web filtering profile.

URI	api/juniper/sd/utm-management/web-filtering-profiles/{id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.web-filtering-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.web-filtering-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the web filtering profile.

### Sample XML Input

```

<web-filtering-profile>
<name>Web-Policy</name>
<description>This is created using REST</description>
<id>128823</id>
<edit-version>1</edit-version>
<safe-search>true</safe-search>
<custom-block-message>This is blocked</custom-block-message>
<quarantine-custom-message>This is blocked</quarantine-custom-message>
<url-category-action-list>
<url-category-action>
<action>BLOCK</action>
<reputation-action/>
</url-category-list>
<id>98368</id>
<name>Enhanced_Abortion</name>
</url-category-list>
</url-category-action>
<url-category-action>
<action>PERMIT</action>
<reputation-action/>
</url-category-list>
<id>98427</id>
<name>Enhanced_Internet_Telephony</name>
</url-category-list>
</url-category-action>
<url-category-action>
<action>QUARANTINE</action>

```

```

<reputation-action/>
<url-category-list>
<id>98422</id>
<name>Enhanced_Pay_to_Surf</name>
</url-category-list>
</url-category-action>
</url-category-action-list>
<site-reputation-actions>
<moderately-safe>PERMIT</moderately-safe>
<harmful>BLOCK</harmful>
<suspicious>LOG_AND_PERMIT</suspicious>
<very-safe>PERMIT</very-safe>
<fairly-safe>LOG_AND_PERMIT</fairly-safe>
</site-reputation-actions>
<default-action>LOG_AND_PERMIT</default-action>
<fallback-default-action>LOG_AND_PERMIT</fallback-default-action>
<profile-type>JUNIPER_ENHANCED</profile-type>
<timeout>15</timeout>
</web-filtering-profile>

```

## DELETE

This request is used to delete web filtering profiles.

URI	api/juniper/sd/utm-management/web-filtering-profiles/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.web-filtering-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.web-filtering-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes web filtering profile.

## PATCH

This request is used to create or modify a web filtering profile.

URI	api/juniper/sd/utm-management/web-filtering-profiles/{id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.utm-management.web-filtering-profile_patch+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.web-filtering-profile_patch+json;version=1;charset=UTF-8
Consumes	None
Produces	Creates or modifies a web filtering profile.

#### Sample XML Input for Adding a New Category

```
<diff>
<add sel="web-filtering-profile/url-category-action-list">
<url-category-action>
<action>LOG_AND_PERMIT</action>
<reputation-action/>
<url-category-list>
<name>Enhanced_Reference_Materials</name>
<id>98438</id>
</url-category-list>
</url-category-action>
</add>
</diff>
```

#### Sample XML Input for Deleting The Category Lists

```
<diff>
<remove
sel="web-filtering-profile/url-category-action-list[url-category-list[name=Enhanced_Reference_Materials]]">
</remove>
</diff>
```

#### Sample XML Input for Replacing With New Sets of Category

```
<diff>
<replace sel="web-filtering-profile/url-category-action-list">
<url-category-action-list>
<url-category-action>
<action>BLOCK</action>
<reputation-action/>
<url-category-list>
<name>Enhanced_Reference_Materials</name>
<id>98438</id>
</url-category-list>
</url-category-action>
</url-category-action-list>
</replace>
</diff>
```

#### Related Documentation

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

## URL Pattern Management RESTful Web Services

---

The following operations can be performed using the Security Director URL Pattern Management RESTful Web Services.

### GET

This request is used to list all the available URL patterns.

URI	/api/juniper/sd/utm-management/url-patterns
HTTP Method	HTTP GET

Content-Type	application/vnd.juniper.sd.utm-management.url-patterns-refs+xml;version=1 application/vnd.juniper.sd.utm-management.url-patterns-refs+json;version=1
Consumes	None
Produces	Collection of URL patterns.

### Sample Input and Output to Get URL Patterns by ID

URI: /api/juniper/sd/utm-management/url-patterns/{id}

**Sample XML Output**

```
url-category-list uri="/api/juniper/sd/utm-management/url-category-lists/99565">
  <name>black-category_1</name>
  <domain-name>Domain-1</domain-name>
  <domain-id>4375</domain-id>
  <id>99565</id>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <profile-type>CUSTOM</profile-type>
  <url-patterns>
    <url-pattern href= "/api/juniper/sd/utm-management/url-patterns/99562" >
      <id>99562</id>
      <domain-id>4375</domain-id>
      <domain-name>Domain-1</domain-name>
      <name>ip-black-list_1</name>
      <moid>
        net.juniper.jnap.sm.policymanager.utm.jpa.EmailAddressPatternEntity:99562
      </moid>
    </url-pattern>
  </url-patterns>
  <created-by-user-name>super</created-by-user-name>
  <last-modified-by-user-name>super</last-modified-by-user-name>
</url-category-list>
```

## POST

This request is used to create a URL pattern.

URI	/api/juniper/sd/utm-management/url-patterns
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.url-patterns+xml;version=1; charset=UTF-8 application/vnd.juniper.sd.utm-management.url-patterns+json;version=1; charset=UTF-8
Consumes	None
Produces	Create a new URL pattern.

**Sample XML Input**

```
<url-pattern>
  <name>Pattern-Block-List</name>
```

```

<description>This object is created using REST</description>
<address-patterns>
  <address-pattern>http://www.test1.com</address-pattern>
  <address-pattern>http://www.test2.com</address-pattern>
  <address-pattern>http://www.test3.com</address-pattern>
</address-patterns>
</url-pattern>

```

## PUT

This request is used to modify the URL pattern.

URI	api/juniper/sd/utm-management/url-patterns/{id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.url-patterns+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.url-patterns+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the URL category.

### Sample XML Input

```

<url-pattern>
  <name>Pattern-Block-List</name>
  <description>This object is created using REST</description>
  <id>128822</id>
  <edit-version>1</edit-version>
  <address-patterns>
    <address-pattern>http://www.test1.com</address-pattern>
    <address-pattern>http://www.test2.com</address-pattern>
    <address-pattern>http://www.test3.com</address-pattern>
  </address-patterns>
</url-pattern>

```

## DELETE

This request is used to delete the URL patterns.

URI	api/juniper/sd/utm-management/url-patterns/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.url-patterns+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.url-patterns+xml;version=1;charset=UTF-8
Consumes	None
Produces	Deletes the URL pattern.

## PATCH

This request is used to create or modify the URL patterns.

URI	api/juniper/sd/utm-management/url-patterns/{id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.utm-management.url-patterns_patch+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.url-patterns_patch+json;version=1;charset=UTF-8
Consumes	None
Produces	Creates or modifies the URL pattern.

**Sample XML Input to Add a New URL List Under URL Pattern**

```
<diff>
  <add sel="url-pattern/address-patterns">
    <address-pattern>http://example.com</address-pattern>
  </add>
</diff>
```

**Sample XML Input to Delete the Existing Lists and Replace With New Lists**

```
<diff>
  <replace sel="url-pattern/address-patterns">
    <address-patterns>
      <address-pattern>http://example1.com</address-pattern>
      <address-pattern>http://example.com</address-pattern>
    </address-patterns>
  </replace>
</diff>
```



**NOTE:** There is no option for deleting URL lists one by one from the existing URL pattern using Patch.

### Related Documentation

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

## URL Category Management RESTful Web Services

The following operations can be performed using the Security Director URL Category Management RESTful Web Services.

## GET

This request is used to list all the available URL category objects.

URI	api/juniper/sd/utm-management/url-category-lists
-----	--

HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.utm-management.url-category-list-refs+xml;version=1 application/vnd.juniper.sd.utm-management.url-category-list-refs+json;version=1
Consumes	None
Produces	Collection of URL category objects.

**Sample XML Output**

```
<url-category-lists uri="/api/juniper/sd/utm-management/url-category-lists"
total="175">
  <url-category-list href="/api/juniper/sd/utm-management/url-category-lists/98319"
uri="/api/juniper/sd/utm-management/url-category-lists/98319">
    <name>Adult_Sexually_Explicit</name>
    <description>Predefined in surf-control server</description>
    <domain-name>SYSTEM</domain-name>
    <domain-id>1</domain-id>
    <id>98319</id>
    <definition-type>PREDEFINED</definition-type>
    <profile-type>SURF_CONTROL</profile-type>
  </url-category-list>
```

**Sample Input and Output to Get URL Category List by ID**

URI: api/juniper/sd/utm-management/url-category-lists/{id}

**Sample XML Output**

```
<url-category-list uri="/api/juniper/sd/utm-management/url-category-lists/99565">
  <name>black-category</name>
  <domain-name>Domain-1</domain-name>
  <domain-id>4375</domain-id>
  <id>99565</id>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <profile-type>CUSTOM</profile-type>
  <url-patterns>
    <url-pattern href="/api/juniper/sd/utm-management/url-patterns/99562" >
      <id>99562</id>
      <domain-id>4375</domain-id>
      <domain-name>Domain-1</domain-name>
      <name>ip-black-list_1</name>
      <moid>
        net.juniper.jnap.sm.policymanager.utm.jp.a.EmailAddressPatternEntity:99562
      </moid>
    </url-pattern>
  </url-patterns>
  <created-by-user-name>super</created-by-user-name>
  <last-modified-by-user-name>super</last-modified-by-user-name>
</url-category-list>
```



## POST

This request is used to create a URL category list.

URI	api/juniper/sd/utm-management/url-category-lists
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.url-category-list+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.url-category-list+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new URL category list.

### Sample XML Input

```
<url-category-list>
  <name>Black-List</name>
  <description>This category created using REST</description>
  <url-patterns>
    <url-pattern>
      <id>128667</id>
      <name>Pattern-1</name>
    </url-pattern>
  </url-patterns>
</url-category-list>
```

## PUT

This request is used to modify the URL category list.

URI	api/juniper/sd/utm-management/url-category-lists/{id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.url-category-list+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.url-category-list+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the URL category.

### Sample XML Input

```
<url-category-list>
  <name>Black-List</name>
  <description>This category created using REST</description>
  <id>128820</id>
  <edit-version>1</edit-version>
  <url-patterns>
    <url-pattern>
      <id>128667</id>
      <name>Pattern-1</name>
    </url-pattern>
  </url-patterns>
</url-category-list>
```

```

    </url-pattern>
  </url-patterns>
</url-category-list>

```

## DELETE

This request is used to delete the URL categories.

URI	api/juniper/sd/utm-management/url-category-lists/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.url-category-list+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.url-category-list+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes the URL category list.

## PATCH

This request is used to create or modify the URL category list.

URI	api/juniper/sd/utm-management/url-category-lists/{id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.utm-management.url-category-list_patch+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.url-category-list_patch+json;version=1;charset=UTF-8
Consumes	None
Produces	Creates or modifies the URL category list.

### Sample XML Input to Add Patterns

```

<diff>
<add sel="url-category-list/url-patterns">
  <url-pattern>
    <name>Pattern-1</name>
    <id>98573</id>
  </url-pattern>
</add>
</diff>

```

### Sample XML Input to Delete URL Patterns

```

<diff>
<remove sel="url-category-list/url-patterns/url-pattern[name='New1']">
</remove>
</diff>

```

**Sample XML Input to Replace With New Sets of URL Patterns**

```
<diff>
<replace sel="url-category-list/url-patterns">
  <url-patterns>
    <url-pattern>
      <name>New1</name>
      <id>98573</id>
    </url-pattern>
  </url-patterns>
</replace>
</diff>
```

**Related Documentation**

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

## Device Profile Management RESTful Web Services

The following operations can be performed using the Security Director Device Profile Management RESTful Web Services.

### GET

This request is used to list all the available device profiles.

URI	/api/juniper/sd/utm-management/utm-device-profiles
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.utm-management.utm-device-profile-refs+xml;version=1;q=0.01 application/vnd.juniper.sd.utm-management.utm-device-profile-refs+json;version=1;q=0.01
Consumes	None
Produces	Collection of device profiles.

**sample XML Output**

```
<utm-device-profiles uri="/api/juniper/sd/utm-management/utm-device-profiles"
total="1">
  <utm-device-profile href=
"/api/juniper/sd/utm-management/utm-device-profiles/121520"
uri="/api/juniper/sd/utm-management/utm-device-profiles/121520">
    <name>Device-1</name>
    <description>Device-1</description>
    <domain-name>Global</domain-name>
    <domain-id>2</domain-id>
    <id>121520</id>
    <definition-type>CUSTOM</definition-type>
  </utm-device-profile>
</utm-device-profiles>
```

**Sample Input and Output to Get Device Profiles by ID**

URI: /api/juniper/sd/utm-management/utm-device-profiles/{id}

**Sample XML output**

```

<utm-device-profile href=
"/api/juniper/sd/utm-management/utm-device-profiles/99580"
uri="/api/juniper/sd/utm-management/utm-device-profiles/99580">
  <name>Global-Settings</name>
  <id>99580</id>
  <definition-type>CUSTOM</definition-type>
  <edit-version>1</edit-version>
  <domain-name>Domain-1</domain-name>
  <domain-id>4375</domain-id>
  <devices
uri="/api/juniper/sd/utm-management/utm-device-profiles/99580/devices"/>
    <as-address-white-list href= "/api/juniper/sd/utm-management/url-patterns/99563"
    >
      <name>ip-white-list_1</name>
      <id>99563</id>
    </as-address-white-list>
    <as-address-black-list href= "/api/juniper/sd/utm-management/url-patterns/99562"
    >
      <name>ip-black-list_1</name>
      <id>99562</id>
    </as-address-black-list>
    <av-mime-white-list>
      <av-mime>image/x-portable-anymap</av-mime>
      <av-mime>video/quicktime</av-mime>
      <av-mime>x-world/x-vrml</av-mime>
    </av-mime-white-list>
    <av-mime-exception-white-list>
      <av-mime-exception>video/quicktime-inappropriate</av-mime-exception>
    </av-mime-exception-white-list>
    <av-url-category-white-list href=
"/api/juniper/sd/utm-management/url-category-lists/99564" >
      <name>white-category_1</name>
      <id>99564</id>
    </av-url-category-white-list>
    <wf-url-category-white-list href=
"/api/juniper/sd/utm-management/url-category-lists/99564" >
      <name>white-category_1</name>
      <id>99564</id>
    </wf-url-category-white-list>
    <wf-url-category-black-list href=
"/api/juniper/sd/utm-management/url-category-lists/99565" >
      <name>black-category_1</name>
      <id>99565</id>
    </wf-url-category-black-list>
    <publish-state>NOT_PUBLISHED</publish-state>
    <created-by-user-name>super</created-by-user-name>
    <last-modified-by-user-name>super</last-modified-by-user-name>
  </utm-device-profile>

```

**POST**

This request is used to create a new device profile.

URI	api/juniper/sd/utm-management/utm-device-profiles
-----	---

HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.utm-management.utm-device-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.utm-device-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Create a new device profile.

**Sample XML Input**

```

<utm-device-profile>
  <name>Global-Setting</name>
  <description>This is created using REST</description>
  <devices uri="/api/juniper/sd/utm-management/utm-device-profiles/121520/devices">

    <device>
      <name>scale-6133</name>
      <moid>net.juniper.jnap.sm.om.jp.a.SecurityDeviceEntity:65624</moid>
    </device>
  </devices>
  <as-address-white-list href= "/api/juniper/sd/utm-management/url-patterns/121511"
>
    <name>Pattern-1</name>
    <id>121511</id>
  </as-address-white-list>
  <as-address-black-list href= "/api/juniper/sd/utm-management/url-patterns/121512"
>
    <name>Pattern-2</name>
    <id>121512</id>
  </as-address-black-list>
  <av-mime-white-list>
    <av-mime>mime1/mime2</av-mime>
    <av-mime>mime3/mime4</av-mime>
  </av-mime-white-list>
  <av-mime-exception-white-list>
    <av-mime-exception>mime2/mime2</av-mime-exception>
    <av-mime-exception>mime3/mime4</av-mime-exception>
  </av-mime-exception-white-list>
  <av-url-category-white-list href=
"/api/juniper/sd/utm-management/url-category-lists/121514" >
    <name>Category-2</name>
    <id>121514</id>
  </av-url-category-white-list>
  <wf-url-category-white-list href=
"/api/juniper/sd/utm-management/url-category-lists/121514" >
    <name>Category-2</name>
    <id>121514</id>
  </wf-url-category-white-list>
  <wf-url-category-black-list href=
"/api/juniper/sd/utm-management/url-category-lists/121514" >
    <name>Category-2</name>
    <id>121514</id>
  </wf-url-category-black-list>
</utm-device-profile>

```

## PUT

This request is used to modify the device profile.

URI	api/juniper/sd/utm-management/utm-device-profiles/{id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.utm-management.utm-device-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.utm-device-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the device profile.

### sample XML Input

```
<utm-device-profile>
  <name>Global-Setting</name>
  <description>This is created using REST</description>
  <edit-version>1</edit-version>
  <id>128830</id>
  <devices
uri="/api/juniper/sd/utm-management/utm-device-profiles/121520/devices">
    <device>
      <name>scale-6133</name>
      <moid>net.juniper.jnap.sm.om.jpa.SecurityDeviceEntity:65624</moid>
    </device>
  </devices>
  <as-address-white-list href= "/api/juniper/sd/utm-management/url-patterns/121511"
>
    <name>Pattern-1</name>
    <id>121511</id>
    </as-address-white-list>
  <as-address-black-list href= "/api/juniper/sd/utm-management/url-patterns/121512"
>
    <name>Pattern-2</name>
    <id>121512</id>
    </as-address-black-list>
    <av-mime-white-list>
      <av-mime>mime1/mime2</av-mime>
      <av-mime>mime3/mime4</av-mime>
    </av-mime-white-list>
    <av-mime-exception-white-list>
      <av-mime-exception>mime2/mime2</av-mime-exception>
      <av-mime-exception>mime3/mime4</av-mime-exception>
    </av-mime-exception-white-list>
    <av-url-category-white-list href=
"/api/juniper/sd/utm-management/url-category-lists/121514" >
      <name>Category-2</name>
      <id>121514</id>
    </av-url-category-white-list>
    <wf-url-category-white-list href=
"/api/juniper/sd/utm-management/url-category-lists/121514" >
      <name>Category-2</name>
```

```

    <id>121514</id>
  </wf-url-category-white-list>
  <wf-url-category-black-list href=
"/api/juniper/sd/utm-management/url-category-lists/121514" >
    <name>Category-2</name>
    <id>121514</id>
  </wf-url-category-black-list>
</utm-device-profile>

```

## DELETE

This request is used to delete the device profile.

URI	api/juniper/sd/utm-management/utm-device-profiles/{id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.utm-management.utm-device-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.utm-management.utm-device-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes the device profile.

### Related Documentation

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)





CHAPTER 9

# Zone Set Management RESTful Web Services

- [Zone Set Management RESTful Web Services on page 91](#)

## Zone Set Management RESTful Web Services

---

The following operations can be performed using the Security Director Zone Set Management RESTful Web Services.

### POST

This request is to create a new zone set.

URI	/api/juniper/sd/zoneset-management/zone-sets/<zone-set id>
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.zoneset-management.zone-set+json;version=1 application/vnd.juniper.sd.zoneset-management.zone-set+xml;version=1
Consumes	None
Produces	Creates a new zone set.

### Sample Zone Set Creation Request Body

Sample XML Input	<pre>&lt;zone-set&gt; &lt;edit-version&gt;1&lt;/edit-version&gt; &lt;zone-type&gt;ZONESET&lt;/zone-type&gt; &lt;zones&gt; internal_1,internal_2,internal_3,internal_4,internal_5 &lt;/zones&gt; &lt;id&gt;&lt;/id&gt; &lt;description&gt;created for testing multizone automation&lt;/description&gt; &lt;domain-id&gt;3&lt;/domain-id&gt; &lt;name&gt;Internal1111&lt;/name&gt; &lt;/zone-set&gt;</pre>
------------------	--

## PUT

This request is to modify the zone set.

URI	/api/juniper/sd/zoneset-management/zone-sets
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.zoneset-management.zone-set+json;version=1 application/vnd.juniper.sd.zoneset-management.zone-set+xml;version=1
Consumes	None
Produces	Modifies a zone set.

### Sample XML Input

```
<zone-set>
<edit-version>3</edit-version>
<zone-type>ZONESET</zone-type>
<zones>
internal_1,internal_2,internal_3,internal_4,internal_5
</zones>
<id>360760</id>
<description>created for testing multizone automation</description>
<name>Internal234234</name>
</zone-set>
```

## DELETE

This request is to delete the zone set.

URI	/api/juniper/sd/zoneset-management/zone-sets/<zone-set id>
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.zoneset-management.zone-set+json;version=1 application/vnd.juniper.sd.zoneset-management.zone-set+xml;version=1
Consumes	None
Produces	Deletes the zone set

### Related Documentation

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

## PART 3

# Security Director Services

- [Firewall Policy Management RESTful Web Services on page 95](#)
- [VPN Management RESTful Web Services on page 129](#)



CHAPTER 10

# Firewall Policy Management RESTful Web Services

- Firewall Policy Management RESTful Web Services on page 95

## Firewall Policy Management RESTful Web Services

The following operations can be performed using the Security Director Firewall Policy Management RESTful Web Services.

### Firewall Policies

#### GET

This request is used to collect all the firewall policies and their associated parameters that are configured in Security Director.

URI	/api/juniper/sd/fwpolicy-management/firewall-policies
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.fwpolicy-management.firewall-policies+xml;version="1" application/vnd.juniper.sd.fwpolicy-management.firewall-policies+JSON;version=1;q=0.01
Consumes	None
Produces	Collection of firewall polices

#### Sample Firewall Policy Management Output

Sample XML Output

```
<fwpolicy-management>
<collection href= "/api/juniper/sd/fwpolicy-management/firewall-policies"
rel="firewall-policies"/>
<collection href= "/api/juniper/sd/fwpolicy-management/policy-profiles"
rel="policy-profiles"/>
<collection href= "/api/juniper/sd/fwpolicy-management/custom-objects"
rel="custom-objects"/>
<collection href= "/api/juniper/sd/fwpolicy-management/custom-columns"
rel="custom-columns"/>
<method href= "/api/juniper/sd/fwpolicy-management/modify-rules"
```

```
rel="modify-rules"/>
<method href= "/api/juniper/sd/fwpolicy-management/publish" rel="publish"/>
</fwpolicy-management>
```

**Sample JSON Output**

```
{
  "fwpolicy-management": {
    "collection": [
      {
        "@href": "/api/juniper/sd/fwpolicy-management/firewall-policies",
        "@rel": "firewall-policies"
      },
      {
        "@href": "/api/juniper/sd/fwpolicy-management/policy-profiles",
        "@rel": "policy-profiles"
      },
      {
        "@href": "/api/juniper/sd/fwpolicy-management/custom-objects",
        "@rel": "custom-objects"
      },
      {
        "@href": "/api/juniper/sd/fwpolicy-management/custom-columns",
        "@rel": "custom-columns"
      }
    ],
    "method": [
      {
        "@href": "/api/juniper/sd/fwpolicy-management/modify-rules",
        "@rel": "modify-rules"
      },
      {
        "@href": "/api/juniper/sd/fwpolicy-management/publish",
        "@rel": "publish"
      }
    ]
  }
}
```

**Sample Firewall Policy Management Input and Output to List Firewall Policies**

URI: /api/juniper/sd/fwpolicy-management/firewall-policies

**Sample XML Output**

```
<firewall-policies uri="/api/juniper/sd/fwpolicy-management/firewall-policies/"
total="3">
  <firewall-policy uri="/api/juniper/sd/fwpolicy-management/firewall-policies/65540"
href= "/api/juniper/sd/fwpolicy-management/firewall-policies/65540" >
    <name>All Devices Policy</name>
    <type>GLOBAL</type>
    <description>Predefined Policy for all devices</description>
    <id>65540</id>
  </firewall-policy>
  <firewall-policy uri="/api/juniper/sd/fwpolicy-management/firewall-policies/65809"
href= "/api/juniper/sd/fwpolicy-management/firewall-policies/65809" >
    <name>test1</name>
    <type>GROUP</type>
    <description>policy created by rest</description>
    <id>65809</id>
```

```

</firewall-policy>
<firewall-policy uri="/api/juniper/sd/fwpolicy-management/firewall-policies/65802"
href= "/api/juniper/sd/fwpolicy-management/firewall-policies/65802" >
<name>test2</name>
<type>GROUP</type>
<description>policy created by rest</description>
<id>65802</id>
</firewall-policy>
</firewall-policies>

```

### Sample Firewall Policy Management Input and Output to Get Policy by ID

URI:/api/juniper/sd/fwpolicy-management/firewall-policies/32772

#### Sample XML Output

```

<firewall-policy uri="/api/juniper/sd/fwpolicy-management/firewall-policies/32772">
<name>All Devices Policy</name>
<last-modified-time>2013-05-09T21:03:32+05:30</last-modified-time>
<created-time>2013-05-09T21:03:32+05:30</created-time>
<definition-type>CUSTOM</definition-type>
<edit-version>0</edit-version>
<policy-type>GLOBAL</policy-type>
<description>Predefined Policy for all devices</description>
<domain-id>2</domain-id>
<policy-state>FINAL</policy-state>
<ips-mode>NONE</ips-mode>
<policy-profile href= "/api/juniper/sd/fwpolicy-management/policy-profiles/32770" >
<id>32770</id>
</policy-profile>
<priority>256</priority>
<ips-sigsets/>
<publish-state>NOT_PUBLISHED</publish-state>
<manage-global-policy>false</manage-global-policy>
<manage-zone-policy>true</manage-zone-policy>
<precedence>-1</precedence>
<policy-priority>LOW</policy-priority>
<id>32772</id>
<rules href=
"/api/juniper/sd/fwpolicy-management/firewall-policies/32772/firewall-rules"
rel="rules"/>
<devices href= "/api/juniper/sd/fwpolicy-management/firewall-policies/32772/devices"
rel="devices"/>
<lock href= "/api/juniper/sd/fwpolicy-management/firewall-policies/32772/lock"
rel="lock"/>
<unlock href= "/api/juniper/sd/fwpolicy-management/firewall-policies/32772/unlock"
rel="unlock"/>
</firewall-policy>

```

#### Sample JSON Output

```

{
  "firewall-policy": {
    "@uri": "/api/juniper/sd/fwpolicy-management/firewall-policies/32772",
    "name": "All Devices Policy",
    "last-modified-time": "2013-05-09T21:03:32+05:30",
    "created-time": "2013-05-09T21:03:32+05:30",
    "definition-type": "CUSTOM",
    "edit-version": 0,
    "policy-type": "GLOBAL",

```

```

    "description": "Predefined Policy for all devices",
    "policy-state": "FINAL",
    "ips-mode": "NONE",
    "policy-profile": {
      "@href": "/api/juniper/sd/fwpolicy-management/policy-profiles/32770",
      "id": 32770
    },
    "priority": 256,
    "ips-sigsets": "",
    "publish-state": "NOT_PUBLISHED",
    "manage-global-policy": false,
    "manage-zone-policy": true,
    "precedence": -1,
    "policy-priority": "LOW",
    "id": 32772,
    "rules": {
      "@href":
"/api/juniper/sd/fwpolicy-management/firewall-policies/32772/firewall-rules",
      "@rel": "rules"
    },
    "devices": {
      "@href": "/api/juniper/sd/fwpolicy-management/firewall-policies/32772/devices",
      "@rel": "devices"
    },
    "lock": {
      "@href": "/api/juniper/sd/fwpolicy-management/firewall-policies/32772/lock",
      "@rel": "lock"
    },
    "unlock": {
      "@href": "/api/juniper/sd/fwpolicy-management/firewall-policies/32772/unlock",
      "@rel": "unlock"
    }
  }
}

```

You can access the associated devices using this href. In case of group policy there will be link to navigate to the device Exception policy and in case of device policy only the device name will be shown.

URI: /api/juniper/sd/fwpolicy-management/firewall-policies/32772/devices

#### Sample XML Output

```

<devices total="2"
uri="/api/juniper/sd/fwpolicy-management/firewall-policies/98325/devices">
  <device href=
"/api/juniper/sd/fwpolicy-management/firewall-policies/327698?device-type=standalone"
  >
    <name>sd-srx210-119.25</name>
  </device>
  <device href=
"/api/juniper/sd/fwpolicy-management/firewall-policies/327694?device-type=standalone"
  >
    <name>sd-srx100-24</name>
  </device>
</devices>

```

#### Sample Firewall Policy Management Input and Output to Get Rule by ID



URI: /api/juniper/sd/fwpolicy-management/firewall-rules/100462

#### Sample XML Output

```
<firewall-rule uri="/api/juniper/sd/fwpolicy-management/firewall-rules/100462">
  <id>100462</id>
  <serial-number>0</serial-number>
  <name>Device-Zone-1</name>
  <source-zones>
    <source-zone>
      <name>trust</name>
      <zone-type>ZONE</zone-type>
      </default-value>
    </source-zone>
  </source-zones>
  <source-addresses>
    <source-address href= "/api/juniper/sd/address-management/addresses/66363">
      <id>66363</id>
      <name>AD1</name>
      <address-type>IPADDRESS</address-type>
    </source-address>
    <source-address href= "/api/juniper/sd/address-management/addresses/66364">
      <id>66364</id>
      <name>AD2</name>
      <address-type>IPADDRESS</address-type>
    </source-address>
  </source-addresses>
  <source-identities>
    <source-identity>role1</source-identity>
    <source-identity>role10</source-identity>
  </source-identities>
  <destination-zones>
    <destination-zone>
      <name>untrust</name>
      <zone-type>ZONE</zone-type>
      </default-value>
    </destination-zone>
  </destination-zones>
  <destination-addresses>
    <destination-address href= "/api/juniper/sd/address-management/addresses/66365">
      <id>66365</id>
      <name>AD3</name>
      <address-type>IPADDRESS</address-type>
    </destination-address>
    <destination-address href= "/api/juniper/sd/address-management/addresses/66366">
      <id>66366</id>
      <name>AD4</name>
      <address-type>IPADDRESS</address-type>
    </destination-address>
  </destination-addresses>
  <services>
    <service href= "/api/juniper/sd/service-management/services/66314" >
      <id>66314</id>
      <name>App1_TCP</name>
    </service>
    <service href= "/api/juniper/sd/service-management/services/66319" >
      <id>66319</id>
      <name>App3_ICMP</name>
```

```
</service>
</services>
<action>TUNNEL</action>
<vpn-tunnel-refs>
<id>32775</id>
<name>sd-srx210-119_25_pv</name>
</vpn-tunnel-refs>
<application-signature-type>NONE</application-signature-type>
<application-signatures/>
<rule-profile>
<custom-profile>
<authentication-type>NONE</authentication-type>
<default-profile>>false</default-profile>
<definition-type>CUSTOM</definition-type>
<destination-address-translation>DROP_TRANSLATED</destination-address-translation>
<enable-count>>true</enable-count>
<id>100463</id>
<infranet-redirect>NONE</infranet-redirect>
<log-at-session-close>>true</log-at-session-close>
<log-at-session-init-time>>true</log-at-session-init-time>
<per-minute-alarm-threshold>4</per-minute-alarm-threshold>
<per-second-alarm-threshold>4</per-second-alarm-threshold>
<redirect>REVERSE_REDIRECT_WX</redirect>
<sd-template>
<id>917596</id>
<name>template2</name>
</sd-template>
<service-offload>>true</service-offload>
<tcp-seq-check>>true</tcp-seq-check>
<tcp-syn-check>>true</tcp-syn-check>
</custom-profile>
<profile-type>CUSTOM</profile-type>
</rule-profile>
<ips-mode>NONE</ips-mode>
<ips-enabled>>false</ips-enabled>
<scheduler>
<id>66672</id>
<name>scheduler1</name>
</scheduler>
<description>description </description>
<custom-column>
<custom-column-value id="66567">asd</custom-column-value>
</custom-column>
<edit-version>3</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>98383</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>sd-srx100-24(Exception)</policy-name>
<enabled>>true</enabled>
<members href=
"/api/juniper/sd/fwpolicy-management/firewall-rules/100462/members"
rel="members"/>
</firewall-rule>
```

### Sample Firewall Policy Management Input and Output with Pagination:

URI:/api/juniper/sd/fwpolicy-management/firewall-policies?paging=(limit eq 10)	The first 10 firewall policies in the first page are listed.
URI:/api/juniper/sd/fwpolicy-management/firewall-policies?paging=(start eq 10, limit eq 5)	Start with record number 10 next 5 records are fetched

### Sample Firewall Policy Management Input and Output with Filtering

URI:/api/juniper/sd/fwpolicy-management/firewall-policies?filter=(global eq 'All')

This policy search is similar to the left pane search of the Security Director policy page. Firewall policy names beginning with *All* are filtered.

#### Sample XML Output

```
<firewall-policies total="1"
uri="/api/juniper/sd/fwpolicy-management/firewall-policies">
  <firewall-policy href="/api/juniper/sd/fwpolicy-management/firewall-policies/32772"
uri="/api/juniper/sd/fwpolicy-management/firewall-policies/32772">
    <name>All Devices Policy</name>
    <type>GLOBAL</type>
    <description>Predefined Policy for all devices</description>
    <id>32772</id>
  </firewall-policy>
</firewall-policies>
```

#### Sample JSON Output

```
{
  "firewall-policies": {
    "@uri": "/api/juniper/sd/fwpolicy-management/firewall-policies",
    "@size": "1",
    "firewall-policy": {
      "@uri": "/api/juniper/sd/fwpolicy-management/firewall-policies/32772",
      "@href": "/api/juniper/sd/fwpolicy-management/firewall-policies/32772",
      "@key": "32772",
      "description": "Predefined Policy for all devices",
      "member-devices": "",
      "name": "All Devices Policy"
    }
  }
}
```

### Sample Firewall Policy Management Input and Output with Sorting

URI:/api/juniper/sd/fwpolicy-management/firewall-policies?sortby=(name(ascending))	All firewall policy names are sorted in an ascending order.
URI:/api/juniper/sd/fwpolicy-management/firewall-policies?sortby=(name(descending))	All firewall policy names are sorted in descending order.

### Sample Firewall Policy Management Input and Output to Get Global or Zone Rule Groups

URI: /api/juniper/sd/fwpolicy-management/firewall-policies/32772/firewall-rules

This request is used to get the global and zone rule groups. This will not list all the members of these rule groups but instead have a href using which the you can fetch all the members of these rule groups. This supports global filtering. This API supports policy right pane search for rule similar to GUI.

**Sample XML Output**

```
<firewall-rules total="2"
uri="/api/juniper/sd/fwpolicy-management/firewall-policies/32772/firewall-rules">
  <firewall-rule href="/api/juniper/sd/fwpolicy-management/firewall-rules/32773"
uri="/api/juniper/sd/fwpolicy-management/firewall-policies/32772/firewall-rules/32773">

    <rule-group-type>ZONE</rule-group-type>
    <rule-type>RULEGROUP</rule-type>
    <name>Zone</name>
    <id>32773</id>
  </firewall-rule>
  <firewall-rule href="/api/juniper/sd/fwpolicy-management/firewall-rules/32776"
uri="/api/juniper/sd/fwpolicy-management/firewall-policies/32772/firewall-rules/32776">

    <rule-group-type>GLOBAL</rule-group-type>
    <rule-type>RULEGROUP</rule-type>
    <name>Global</name>
    <id>32776</id>
  </firewall-rule>
</firewall-rules>
```

URI:

/api/juniper/sd/fwpolicy-management/firewall-policies/32779/firewall-rules?filter=(global eq 'trust'). This URI returns only those rule group under which the desired rule is present.

URI: /api/juniper/sd/fwpolicy-management/firewall-rules/32781/members?filter=(global eq 'trust'). To fetch the exact rule you can use filter for the rule members.

**Sample Firewall Policy Management Input and Output to Rule or Rule Groups by ID**

URI:/api/juniper/sd/fwpolicy-management/firewall-rules/32778

This request is used to get rules by rule ID. Rule groups list information only pertaining to the rule group but it does not list all the members of the rule group. For the rule group members, href is provided to get all the members of the rule group. Rules contain the information such as rule name, source and destination address, source and destination zones, action, application firewall, rule profile, and so on.

**Sample XML Ouput**

```
<firewall-rule uri="/api/juniper/sd/fwpolicy-management/firewall-rules/32778">
  <id>32778</id>
  <serial-number>0</serial-number>
  <name>All Devices Post Rules</name>
  <source-zone/>
  <source-addresses/>
  <sourceidentities/>
  <destination-zone/>
  <destination-addresses/>
  <vpn-tunnel-refs/>
  <application-signature-type>NONE</application-signature-type>
  <application-signatures/>
  <rule-profile>
```

```

    <profile-type>INHERITED</profile-type>
  </rule-profile>
  <ips-mode>NONE</ips-mode>
  <ips-enabled>>false</ips-enabled>
  <scheduler/>
  <custom-column/>
  <edit-version>0</edit-version>
  <definition-type>CUSTOM</definition-type>
  <rule-group-type>POST</rule-group-type>
  <rule-group-id>32776</rule-group-id>
  <rule-type>RULEGROUP</rule-type>
  <rule-order>1</rule-order>
  <policy-name>All Devices Policy</policy-name>
  <enabled>>true</enabled>
  <members
href="/api/juniper/sd/fwpolicy-management/firewall-rules/32778/members" rel=""/>

</firewall-rule>

```

### Sample Firewall Policy Management Input and Output to Get Rule Group Members

URI: `/api/juniper/sd/fwpolicy-management/firewall-policies/65547/firewall-rules/65549/members`

This API is used to all the members of a rule group or rules under a rule group with the rule ID.

#### Sample XML Output

```

<firewall-rules total="3"
uri="/api/juniper/sd/fwpolicy-management/firewall-rules/32774/members">
  <firewall-rule href= "/api/juniper/sd/fwpolicy-management/firewall-rules/2195456"
uri="/api/juniper/sd/fwpolicy-management/firewall-rules/32774/members/2195456">
    <rule-group-type>CUSTOM</rule-group-type>
    <rule-type>RULE</rule-type>
    <name>All-Devices-Zone-Pre-1</name>
    <id>2195456</id>
  </firewall-rule>
  <firewall-rule href= "/api/juniper/sd/fwpolicy-management/firewall-rules/2195458"
uri="/api/juniper/sd/fwpolicy-management/firewall-rules/32774/members/2195458">
    <rule-group-type>CUSTOM</rule-group-type>
    <rule-type>RULE</rule-type>
    <name>All-Devices-Zone-Pre-2</name>
    <id>2195458</id>
  </firewall-rule>
  <firewall-rule href= "/api/juniper/sd/fwpolicy-management/firewall-rules/2195459"
uri="/api/juniper/sd/fwpolicy-management/firewall-rules/32774/members/2195459">
    <rule-group-type>CUSTOM</rule-group-type>
    <rule-type>RULE</rule-type>
    <name>All-Devices-Zone-Pre-3</name>
    <id>2195459</id>
  </firewall-rule>
</firewall-rules>

```

### Custom Column and Custom Objects

This request is used to query for custom columns of the firewall policy.

URI: `/api/juniper/sd/fwpolicy-management/custom-columns`

**Sample XML Output**

```
<custom-columns total="3"
uri="/api/juniper/sd/fwpolicy-management/custom-columns">
  <custom-column>
    <created-by-user-name>super</created-by-user-name>
    <created-time>2013-05-21T07:47:43Z</created-time>
    <edit-version>0</edit-version>
    <id>66567</id>
    <last-modified-time>2013-05-21T10:12:55Z</last-modified-time>
    <name>column1</name>
    <regex>[A-Z]</regex>
  </custom-column>
  <custom-column>
    <created-by-user-name>super</created-by-user-name>
    <created-time>2013-05-21T10:12:31Z</created-time>
    <edit-version>0</edit-version>
    <id>66676</id>
    <last-modified-time>2013-05-21T10:12:31Z</last-modified-time>
    <name>column2</name>
    <regex>[/d/d/d]</regex>
  </custom-column>
  <custom-column>
    <created-by-user-name>super</created-by-user-name>
    <created-time>2013-05-21T10:12:44Z</created-time>
    <edit-version>0</edit-version>
    <id>66677</id>
    <last-modified-time>2013-05-21T10:12:44Z</last-modified-time>
    <name>column3</name>
    <regex>[1-9]</regex>
  </custom-column>
</custom-columns>
```

This request is used to query for custom objects of the firewall policy.

URI: /api/juniper/sd/fwpolicy-management/custom-objects

**Sample XML Output**

```
<custom-objects total="4">
  <custom-object>
    <device-families>
      <device-family>junos-es</device-family>
    </device-families>
    <os-version>12.1R3.5</os-version>
    <state>enabled</state>
    <metadata/>
    <name>temp1</name>
    <description/>
    <last-updated-by>vpsahu</last-updated-by>
    <last-update-time>1369047070167</last-update-time>
    <schema-id>template-720958</schema-id>
    <config-type>CONFIG_TEMPLATE</config-type>
  </custom-object>
  <custom-object>
    <device-families>
      <device-family>junos-ex</device-family>
    </device-families>
    <os-version>12.1R3.5</os-version>
    <state>enabled</state>
```

```

<metadata/>
<name>temp2</name>
<description>sad asd </description>
<last-updated-by>vpsahu</last-updated-by>
<last-update-time>1369047081773</last-update-time>
<schema-id>template-287296</schema-id>
<config-type>CONFIG_TEMPLATE</config-type>
</custom-object>
<custom-object>
<device-families>
<device-family>junos-es</device-family>
</device-families>
<os-version>12.1R3.5</os-version>
<state>enabled</state>
<metadata/>
<name>template1</name>
<description>asda sd</description>
<last-updated-by>super</last-updated-by>
<last-update-time>1369122517597</last-update-time>
<schema-id>template-720958</schema-id>
<config-type>CONFIG_TEMPLATE</config-type>
</custom-object>
<custom-object>
<device-families>
<device-family>junos-es</device-family>
</device-families>
<os-version>12.1R3.5</os-version>
<state>enabled</state>
<metadata/>
<name>template2</name>
<description>ads asd a</description>
<last-updated-by>super</last-updated-by>
<last-update-time>1369125742772</last-update-time>
<schema-id>template-720965</schema-id>
<config-type>CONFIG_TEMPLATE</config-type>
</custom-object>
</custom-objects>

```

## POST

This request is used to create a new firewall policy. you must provide all the basic information of the policy such as policy name, priority, precedence, profile, IPS configuration mode, and so on. You can provide the list of assigned devices to this policy. Otherwise, you can assign a new device to the policy or remove the existing device from the list, by using Assign Devices API.

URI	/api/juniper/sd/fwpolicy-management/firewall-policies
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.fwpolicy-management.firewall-policy+xml;version=1; charset=UTF-8 application/vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1; charset=UTF-8

Consumes	None
Produces	Creates a new firewall policy

To create a new firewall policy:

1. Send the new policy information to the device, as shown in the following example.  
Copy this information in the Body window, and click **SEND**.

#### Sample XML Input

```
<firewall-policy>
  <name>GroupPolicy</name>
  <definition-type>CUSTOM</definition-type>
  <policy-type>GROUP</policy-type>
  <description>policy created by rest</description>
  <policy-state>FINAL</policy-state>
  <ips-mode>NONE</ips-mode>
  <ips-sigsets/>
  <member-devices/>
  <policy-profile>
    <id>32768</id>
  </policy-profile>
  <priority>65539</priority>
  <publish-state>NOT_PUBLISHED</publish-state>
  <manage-global-policy>>false</manage-global-policy>
  <manage-zone-policy>true</manage-zone-policy>
  <precedence>3</precedence>
  <policy-priority>LOW</policy-priority>
  <rules/>
</firewall-policy>
```

You can query for the profile ID of the policy using GET method.

The following example shows creating firewall policy with IPS mode as Basic. Copy this snippet in the Body window and send it to the device.

#### Sample XML Input

```
<firewall-policy>
  <name>GP_IPS_BASIC_REST</name>
  <edit-version>0</edit-version>
  <definition-type>CUSTOM</definition-type>
  <created-by-user-name>super</created-by-user-name>
  <last-modified-by-user-name />
  <id />
  <policy-type>GROUP</policy-type>
  <description>Policy Created using REST API</description>
  <policy-state>FINAL</policy-state>
  <ips-mode>BASIC</ips-mode>
  <policy-profile>
    <id>32769</id>
  </policy-profile>
  <priority>65537</priority>
  <publish-state>NOT_PUBLISHED</publish-state>
  <manage-global-policy>true</manage-global-policy>
  <manage-zone-policy>true</manage-zone-policy>
```



```

<precedence>1</precedence>
<policy-priority>LOW</policy-priority>
<ips-sigsets>
  <ips-sigset>
    <name>Web_Server (Predefined)</name>
    <id>232471</id>
  </ips-sigset>
  <ips-sigset>
    <name>DMZ_Services (Predefined)</name>
    <id>232472</id>
  </ips-sigset>
  <ips-sigset>
    <name>File_Server (Predefined)</name>
    <id>232473</id>
  </ips-sigset>
</ips-sigsets>
</firewall-policy>

```

### ***Locking and Unlocking a Firewall Policy***

This request is used to lock a policy before modifying the policy. Once you complete with the modification, you must unlock the policy. There is a lock time-out before which you must unlock the policy, otherwise the policy is automatically unlocked after the time-out value. The time out is reset on every operation on a policy. If there is no operation, the lock times out occurs

Before you modify, delete a policy, modify rules, or assigning devices, you must first the lock policy. After editing the policy and saving the changes, you must unlock the policy.

URI	/api/juniper/sd/fwpolicy-management/firewall-policies/{policy-id}/lock
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.lock-management.lock+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.lock-management.lock+jsonl;version=1;charset=UTF-8
Consumes	None
Produces	Locks the firewall policy

To unlock a locked policy, send URI:

/api/juniper/sd/fwpolicy-management/firewall-policies/{policy-id}/unlock to the device.

### ***Publish Firewall Policy***

This request is used to schedule job and publish a policy. To get the job notifications at each stage, you must create a job queue, a consumer for this queue, and pass the queue name as the query parameter. Once the consumer for the queue is created, you can pull the job message from the queue using the consumer. The job message contains the

information such as percentage of completion, status of the job, and summary of the job result. It is not required to lock the policy to publish a policy.

URI	/api/juniper/sd/fwpolicy-management/publish
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.fwpolicy-management.publish+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.fwpolicy-management.publish+json;version=1;charset=UTF-8
Consumes	None
Produces	Publishes the firewall policy

To publish a policy:

1. Send the publish information in the Body window, as shown in the following example.

#### Sample XML Input

```
<publish>
  <policy-ids>
    <policy-id>
      1376291
    </policy-id>
  </policy-ids>
</publish>
```

2. To publish and update the policy, use the URI:  
/api/juniper/sd/fwpolicy-management/publish?update=true.

#### Sample Firewall Policy Management Input for Scheduling of Publish Operation

URI: /api/juniper/sd/fwpolicy-management/publish?schedule=(at(01 01 11 26 05 ? 2013))

The syntax for scheduling a publish at a particular time is schedule= (at(ss mm HH dd MM ? yy)).

- ss—Seconds (mandatory field)
- mm—Minutes (mandatory field)
- HH—Hours (mandatory field)
- dd—Day of the month (mandatory field)
- EE—Day of week (mandatory field)
- MM—Month (mandatory field)
- yy—Year (optional field)
- ?—This is the allowed value of EE.

If you want to schedule the update after a particular time, send the information as shown in the following example.

URI: /api/juniper/sd/ fwpolicy-management/publish?schedule=(after(00 00 30))

The syntax for scheduling after a particular time period is schedule=(after(dd HH mm)) or schedule=(after(HH mm)).

- dd—Days (optional parameter)
- HH—Hours
- mm—Minutes

### ***Assign Devices to Firewall Policy***

This request is used to assign devices to a policy or remove the devices from a policy. You are required to send the list of devices, and this list replaces the existing list of devices. You must lock the policy before assigning devices.

URI	/api/juniper/sd/fwpolicy-management/firewall-policies/{policy-id}/assign-devices
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.fwpolicy-management.assign-devices+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.fwpolicy-management.assign-devices+json;version=1;charset=UTF-8
Consumes	None
Produces	Assigns devices to the firewall policy

The following example shows assigning devices to the policy. Copy this information in the Body window, send it to the device.

#### **Sample XML Input**

```
<assign-devices>
<deleted-devices>
<deleted-device>
<name>SN-srx3600-1</name>
<moid>net.juniper.jmp.jpa.LogicalDevice:327734</moid>
</deleted-device>
</deleted-devices>
</assign-devices>
```

#### **Sample XML Input to Add Devices to Policy**

```
<assign-devices>
<added-devices>
<added-device>
<moid>net.juniper.jnap.sm.om.jpa.SecurityDeviceEntity:99118</moid>
</added-device>
</added-devices>
</assign-devices>
```

**Adding And Modifying Rules**

This request is used to add a rule or modify the existing rules.

URI	/api/juniper/sd/fwpolicy-management/modify-rules
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.fwpolicy-management.modify-rules+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.fwpolicy-management.modify-rules+json;version=1;charset=UTF-8
Consumes	None
Produces	Adds a new rule or modifies the existing rules

To add a new rule, send the new rule information in the Body window, as shown in the following example.

**Sample XML Input**

```
<modify-rules>
<edit-version>6</edit-version>
<policy-id>1081361</policy-id>
<added-rules>
<added-rule>
<serial-number>0</serial-number>
<name>GroupPolicy-Zone-Pre-2</name>
<source-zones>
<source-zone>
<name>untrust</name>
<zone-type>ZONE</zone-type>
</default-value>
</source-zone>
</source-zones>
<source-addresses>
<id>1016076</id>
<name>10.159.2.0/25</name>
<address-type>NETWORK</address-type>
</source-address>
</source-addresses>
<source-identities>
<source-identity>Authenticated-User</source-identity>
</source-identities>
<destination-zones>
<destination-zone>
<name>VPN</name>
<zone-type>ZONE</zone-type>
</destination-zone>
</destination-zones>
<destination-addresses>
<id>1016100</id>
<name>10.159.3.0/24</name>
<address-type>NETWORK</address-type>
</destination-address>
</destination-addresses>
```

```

<services>
<id>98674</id>
<name>apple-ichat</name>
</service>
</services>
<action>PERMIT</action>
<vpn-tunnel-refs/>
<application-signature-type>BLACKLIST</application-signature-type>
<application-signatures>
<id>3792</id>
<name>163</name>
</application-signature>
<id>5502</id>
<name>2CH</name>
</application-signature>
</application-signatures>
<rule-profile>
<profile-type>INHERITED</profile-type>
</rule-profile>
<ips-mode>BASIC</ips-mode>
<ips-enabled>>false</ips-enabled>
<scheduler>
<id>98969</id>
<name>sc5</name>
</scheduler>
<description>desc</description>
<custom-column>
<custom-column-value id="1016232">asd</custom-column-value>
</custom-column>
<edit-version>5</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>1081363</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>GroupPolicy</policy-name>
<enabled>>true</enabled>
</added-rule>
</added-rules>
</modify-rules>

```

If you want make Action as Tunnel, send the following information, in the place of Action configuration.

```

<action>TUNNEL</action>
<vpn-tunnel-refs>
<id>622595</id>
<name>sd-srx210-119_25_pbv</name>
</vpn-tunnel-refs>

```

To modify rules, add the necessary information similar to the configuration parameters sent to add a rule between <modified-rules><modified-rule> tags.

To delete any rule ID, send the delete information as shown in the following example.

**Sample XML Input**

```
<modify-rules>
  <edit-version>17</edit-version>
  <policy-id>1015862</policy-id>
  <deleted-rules>
    <deleted-rule>1015881</deleted-rule>
  </deleted-rules>
</modify-rules>
```

**Sample Input to add a New Rule with Security Intelligence Policy****Sample XML Input**

```
<firewall-policy>
  <modify-rules>
    <edit-version>0</edit-version>
    <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
    <added-rules>
      <added-rule>
        <id></id>
        <serial-number>0</serial-number>
        <name>Rule-1</name>
        <source-zones>
          <source-zone>
            <name>trust</name>
            <zone-type>ZONE</zone-type>
          </source-zone>
        </source-zones>
        <source-addresses>
          <source-address>
            <id>0000addresses?include-dynamic-addresses=true-Dynamic-add1</id>
            <name>Dynamic-add1</name>
            <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
          </source-address>
          <source-excluded-address>>false</source-excluded-address>
        </source-addresses>
        <source-identities />
        <destination-zones>
          <destination-zone>
            <name>untrust</name>
            <zone-type>ZONE</zone-type>
          </destination-zone>
        </destination-zones>
        <destination-addresses>
          <destination-address>
            <id>0000addresses-Any</id>
            <name>Any</name>
            <address-type>ANY</address-type>
          </destination-address>
        </destination-addresses>
        <destination-excluded-address>>false</destination-excluded-address>
      </added-rule>
    </added-rules>
  </modify-rules>
  <action>PERMIT</action>
  <vpn-tunnel-refs />
</firewall-policy>
```

```

<application-signature-type>NONE</application-signature-type>
<application-signatures />
<rule-profile>
  <profile-type>INHERITED</profile-type>
</rule-profile>
<ips-mode>ADVANCED</ips-mode>
<ips-enabled>>false</ips-enabled>
<scheduler />
<utm-policy />
<secintel-policy>
  <id>0000secintel-policies-Secintelpolicy-1</id>
  <name>Secintelpolicy-1</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>>true</enabled>
<members />
</added-rule>
</added-rules>
</modify-rules>

<modify-rules>
  <edit-version>1</edit-version>
  <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
  <added-rules>
    <added-rule>
      <id>36833</id>
      <serial-number>0</serial-number>
      <name>Rule-2</name>
      <source-zones>
        <source-zone>
          <name>trust</name>
          <zone-type>ZONE</zone-type>
        </source-zone>
      </source-zones>
      <source-addresses>
        <source-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add3</id>
          <name>Dynamic-add1</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </source-address>
      </source-addresses>
      <source-excluded-address>>false</source-excluded-address>
      <source-identities />
      <destination-zones>
        <destination-zone>
          <name>untrust</name>
          <zone-type>ZONE</zone-type>
        </destination-zone>
      </destination-zones>
    </added-rule>
  </added-rules>
</modify-rules>

```

```
<destination-addresses>
  <destination-address>
    <id>0000addresses?include-dynamic-addresses=true-Dynamic-add1</id>
    <name>Dynamic-add1</name>
    <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
  </destination-address>
</destination-addresses>
<destination-excluded-address>false</destination-excluded-address>
<services>
  <service>
    <id>0000services-Any</id>
    <name>Any</name>
  </service>
</services>
<action>PERMIT</action>
<vpn-tunnel-refs />
<application-signature-type>NONE</application-signature-type>
<application-signatures />
<rule-profile>
  <profile-type>INHERITED</profile-type>
</rule-profile>
<ips-mode>ADVANCED</ips-mode>
<ips-enabled>false</ips-enabled>
<scheduler />
<utm-policy />
<secintel-policy>
  <id>0000secintel-policies-Secintelpolicy-2</id>
  <name>Secintelpolicy-2</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>true</enabled>
<members />
</added-rule>
</added-rules>
</modify-rules>

<modify-rules>
  <edit-version>2</edit-version>
  <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
  <added-rules>
    <added-rule>
      <id>36833</id>
      <serial-number>0</serial-number>
      <name>Rule-3</name>
      <source-zones>
        <source-zone>
          <name>trust</name>
          <zone-type>ZONE</zone-type>
        </source-zone>
```



```

</source-zones>
<source-addresses>
  <source-address>
    <id>0000addresses?include-dynamic-addresses=true-Dynamic-add1</id>
    <name>Dynamic-add1</name>
    <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
  </source-address>
</source-addresses>
<source-excluded-address>>false</source-excluded-address>
<source-identities />
<destination-zones>
  <destination-zone>
    <name>untrust</name>
    <zone-type>ZONE</zone-type>
  </destination-zone>
</destination-zones>
<destination-addresses>
  <destination-address>
    <id>0000addresses?include-dynamic-addresses=true-Dynamic-add2</id>
    <name>Dynamic-add2</name>
    <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
  </destination-address>
</destination-addresses>
<destination-excluded-address>>false</destination-excluded-address>
<services>
  <service>
    <id>0000services-Any</id>
    <name>Any</name>
  </service>
</services>
<action>PERMIT</action>
<vpn-tunnel-refs />
<application-signature-type>NONE</application-signature-type>
<application-signatures />
<rule-profile>
  <profile-type>INHERITED</profile-type>
</rule-profile>
<ips-mode>ADVANCED</ips-mode>
<ips-enabled>>false</ips-enabled>
<scheduler />
<utm-policy />
<secintel-policy>
  <id>0000secintel-policies-Secintelpolicy-3</id>
  <name>Secintelpolicy-3</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>>true</enabled>
<members />
</added-rule>

```

```
</added-rules>
</modify-rules>

<modify-rules>
  <edit-version>3</edit-version>
  <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
  <added-rules>
    <added-rule>
      <serial-number>0</serial-number>
      <name>Rule-4</name>
      <source-zones>
        <source-zone>
          <name>trust</name>
          <zone-type>ZONE</zone-type>
        </source-zone>
      </source-zones>
      <source-addresses>
        <source-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add3</id>
          <name>Dynamic-add3</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </source-address>
      </source-addresses>
      <source-excluded-address>false</source-excluded-address>
      <source-identities />
      <destination-zones>
        <destination-zone>
          <name>untrust</name>
          <zone-type>ZONE</zone-type>
        </destination-zone>
      </destination-zones>
      <destination-addresses>
        <destination-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add2</id>
          <name>Dynamic-add2</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </destination-address>
      </destination-addresses>
      <destination-excluded-address>false</destination-excluded-address>
      <services>
        <service>
          <id>0000services-aol</id>
          <name>aol</name>
        </service>
      </services>
      <action>PERMIT</action>
      <vpn-tunnel-refs />
      <application-signature-type>NONE</application-signature-type>
      <application-signatures />
      <rule-profile>
        <profile-type>INHERITED</profile-type>
      </rule-profile>
      <ips-mode>ADVANCED</ips-mode>
      <ips-enabled>false</ips-enabled>
      <scheduler />
      <utm-policy />
    </added-rule>
  </added-rules>
</modify-rules>
```

```

<secintel-policy>
  <id>0000secintel-policies-Secintelpolicy-4</id>
  <name>Secintelpolicy-4</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>true</enabled>
<members />
</added-rule>
</added-rules>
</modify-rules>

<modify-rules>
  <edit-version>4</edit-version>
  <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
  <added-rules>
    <added-rule>
      <serial-number>0</serial-number>
      <name>Rule-5</name>
      <source-zones>
        <source-zone>
          <name>trust</name>
          <zone-type>ZONE</zone-type>
        </source-zone>
      </source-zones>
      <source-addresses>
        <source-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add2</id>
          <name>Dynamic-add2</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </source-address>
      </source-addresses>
      <source-excluded-address>>false</source-excluded-address>
      <source-identities />
      <destination-zones>
        <destination-zone>
          <name>untrust</name>
          <zone-type>ZONE</zone-type>
        </destination-zone>
      </destination-zones>
      <destination-addresses>
        <destination-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add3</id>
          <name>Dynamic-add3</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </destination-address>
      </destination-addresses>
      <destination-excluded-address>>false</destination-excluded-address>
      <services>
        <service>

```

```
<id>0000services-bgp</id>
<name>bgp</name>
</service>
</services>
<action>PERMIT</action>
<vpn-tunnel-refs />
<application-signature-type>NONE</application-signature-type>
<application-signatures />
<rule-profile>
  <profile-type>INHERITED</profile-type>
</rule-profile>
<ips-mode>ADVANCED</ips-mode>
<ips-enabled>>false</ips-enabled>
<scheduler />
<utm-policy />
<secintel-policy>
  <id>0000secintel-policies-Secintelpolicy-5</id>
  <name>Secintelpolicy-5</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>>true</enabled>
<members />
</added-rule>
</added-rules>
</modify-rules>
<modify-rules>
  <edit-version>5</edit-version>
  <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
  <added-rules>
    <added-rule>
      <serial-number>0</serial-number>
      <name>Rule-6</name>
      <source-zones>
        <source-zone>
          <name>untrust</name>
          <zone-type>ZONE</zone-type>
        </source-zone>
      </source-zones>
      <source-addresses>
        <source-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add3</id>
          <name>Dynamic-add3</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </source-address>
      </source-addresses>
      <source-excluded-address>>false</source-excluded-address>
      <source-identities />
      <destination-zones>
        <destination-zone>
```

```

    <name>trust</name>
    <zone-type>ZONE</zone-type>
  </destination-zone>
</destination-zones>
<destination-addresses>
  <destination-address>
    <id>0000addresses?include-dynamic-addresses=true-Dynamic-add1</id>
    <name>Dynamic-add1</name>
    <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
  </destination-address>
</destination-addresses>
<destination-excluded-address>false</destination-excluded-address>
<services>
  <service>
    <id>0000services-Any</id>
    <name>Any</name>
  </service>
</services>
<action>PERMIT</action>
<vpn-tunnel-refs />
<application-signature-type>NONE</application-signature-type>
<application-signatures />
<rule-profile>
  <profile-type>INHERITED</profile-type>
</rule-profile>
<ips-mode>ADVANCED</ips-mode>
<ips-enabled>false</ips-enabled>
<scheduler />
<utm-policy />
<secintel-policy>
  <id>0000secintel-policies-Secintelpolicy-6</id>
  <name>Secintelpolicy-6</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>true</enabled>
<members />
</added-rule>
</added-rules>
</modify-rules>
<modify-rules>
  <edit-version>6</edit-version>
  <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
  <added-rules>
    <added-rule>
      <serial-number>0</serial-number>
      <name>Rule-7</name>
      <source-zones>
        <source-zone>
          <name>untrust</name>

```

```
<zone-type>ZONE</zone-type>
</source-zone>
</source-zones>
<source-addresses>
<source-address>
<id>0000addresses?include-dynamic-addresses=true-Dynamic-add1</id>
<name>Dynamic-add1</name>
<address-type>DYNAMIC_ADDRESS_GROUP</address-type>
</source-address>
</source-addresses>
<source-excluded-address>>false</source-excluded-address>
<source-identities />
<destination-zones>
<destination-zone>
<name>trust</name>
<zone-type>ZONE</zone-type>
</destination-zone>
</destination-zones>
<destination-addresses>
<destination-address>
<id>0000addresses?include-dynamic-addresses=true-Dynamic-add2</id>
<name>Dynamic-add2</name>
<address-type>DYNAMIC_ADDRESS_GROUP</address-type>
</destination-address>
</destination-addresses>
<destination-excluded-address>>false</destination-excluded-address>
<services>
<service>
<id>0000services-Any</id>
<name>Any</name>
</service>
</services>
<action>PERMIT</action>
<vpn-tunnel-refs />
<application-signature-type>NONE</application-signature-type>
<application-signatures />
<rule-profile>
<profile-type>INHERITED</profile-type>
</rule-profile>
<ips-mode>ADVANCED</ips-mode>
<ips-enabled>>false</ips-enabled>
<scheduler />
<utm-policy />
<secintel-policy>
<id>0000secintel-policies-Secintelpolicy-7</id>
<name>Secintelpolicy-7</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>>true</enabled>
```

```

    <members />
  </added-rule>
</added-rules>
</modify-rules>
<modify-rules>
  <edit-version>7</edit-version>
  <policy-id>0000firewall-policies-FW-POLICY-SecIntel1</policy-id>
  <added-rules>
    <added-rule>
      <serial-number>0</serial-number>
      <name>Rule-8</name>
      <source-zones>
        <source-zone>
          <name>untrust</name>
          <zone-type>ZONE</zone-type>
        </source-zone>
      </source-zones>
      <source-addresses>
        <source-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add2</id>
          <name>Dynamic-add2</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </source-address>
      </source-addresses>
      <source-excluded-address>>false</source-excluded-address>
      <source-identities />
      <destination-zones>
        <destination-zone>
          <name>trust</name>
          <zone-type>ZONE</zone-type>
        </destination-zone>
      </destination-zones>
      <destination-addresses>
        <destination-address>
          <id>0000addresses?include-dynamic-addresses=true-Dynamic-add3</id>
          <name>Dynamic-add3</name>
          <address-type>DYNAMIC_ADDRESS_GROUP</address-type>
        </destination-address>
      </destination-addresses>
      <destination-excluded-address>>false</destination-excluded-address>
      <services>
        <service>
          <id>0000services-Any</id>
          <name>Any</name>
        </service>
      </services>
      <action>PERMIT</action>
      <vpn-tunnel-refs />
      <application-signature-type>NONE</application-signature-type>
      <application-signatures />
      <rule-profile>
        <profile-type>INHERITED</profile-type>
      </rule-profile>
      <ips-mode>ADVANCED</ips-mode>
      <ips-enabled>>false</ips-enabled>
    </added-rule>
  </modify-rules>
</scheduler />

```

```

<utm-policy />
<secintel-policy>
  <id>0000secintel-policies-Secintelpolicy-8</id>
  <name>Secintelpolicy-8</name>
</secintel-policy>
<custom-column />
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<rule-group-type>CUSTOM</rule-group-type>
<rule-group-id>0000FW-POLICY-SecIntel1-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>l
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntel1</policy-name>
<enabled>true</enabled>
<members />
</added-rule>
</added-rules>
</modify-rules>
</firewall-policy>

```

## PUT

This request is used to modify an existing firewall policy. The Modify operation is a full replace and therefore, you must provide all the basic information of a policy irrespective of that particular field has a new value or not.

URI	/api/juniper/sd/fwpolicy-management/firewall-policies/{policy-id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.fwpolicy-management.firewall-policy+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies any firewall policy

To modify a policy:

1. Send the modification information to the device, as shown in the following example. Copy this information in the Body window, and click **SEND**.

### Sample XML Input

```

<firewall-policy
uri="/api/juniper/sd/fwpolicy-management/firewall-policies/1081361">
  <name>GroupPolicy1</name>
  <last-modified-time>2013-04-24T23:32:42+05:30</last-modified-time>
  <created-time>2013-04-24T23:29:11+05:30</created-time>
  <created-by-user-name>super</created-by-user-name>
  <definition-type>CUSTOM</definition-type>
  <edit-version>0</edit-version>
  <policy-type>GROUP</policy-type>

```



```

<description>policy created by rest</description>
<policy-state>FINAL</policy-state>
<ips-mode>BASIC</ips-mode>
<policy-profile
href="/api/juniper/sd/fwpolicy-management/policy-profiles/32768">
  <id>32768</id>
</policy-profile>
<priority>65537</priority>
<ips-sigsets>
  <ips-sigset href="/api/juniper/sd/ips-management/ips-sig-sets/232473">
    <id>232473</id>
    <name>Web_Server (Predefined)</name>
  </ips-sigset>
  <ips-sigset href="/api/juniper/sd/ips-management/ips-sig-sets/232481">
    <id>232481</id>
    <name>DMZ_Services (Predefined)</name>
  </ips-sigset>
  <ips-sigset href="/api/juniper/sd/ips-management/ips-sig-sets/232523">
    <id>232523</id>
    <name>Recommended (Predefined)</name>
  </ips-sigset>
</ips-sigsets>
<member-devices/>
<utm-policy>
  <id>12345</id>
  <name>UTM_Policy-1</name>
</utm-policy>
<publish-state>NOT_PUBLISHED</publish-state>
<manage-global-policy>>false</manage-global-policy>
<manage-zone-policy>>true</manage-zone-policy>
<precedence>1</precedence>
<policy-priority>LOW</policy-priority>
<id>1081361</id>
<rules
href="/api/juniper/sd/fwpolicy-management/firewall-policies/1081361/firewall-rules"
rel="Rules in the policy"/>
</firewall-policy>

```

2. The required fields are modified for a policy.

## DELETE

This request is used to delete an existing policy. You must lock the policy before deleting.

URI	/api/juniper/sd/fwpolicy-management/{policy-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.fwpolicy-management.firewall-policy+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes a policy

## Policy Profiles

### GET

The Security Director Policy Profile Management RESTful Web Service is used to collect all the policy profiles.

URI	/api/juniper/sd/fwpolicy-management/policy-profiles
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.fwpolicy-management.policy-profiles+xml;version=1;q=0.01 application/vnd.juniper.sd.fwpolicy-management.policy-profiles+json;version=1;q=0.01
Consumes	None
Produces	Collection of policy profiles

### Sample Policy Profile Management Input and Output to Get Policy Profile by ID

URI:/api/juniper/sd/fwpolicy-management/policy-profiles/32769

This API is used to get the policy profile used in the rule with a profile ID. Link for the user defined profile is available only in the rule. For Custom Profile, details are shown in the rule itself. The rule-profile tag is used for the policy profile.

#### Sample XML Output

```
<policy-profile uri="/api/juniper/sd/fwpolicy-management/policy-profiles/32769">
  <edit-version>0</edit-version>
  <definition-type>PREDEFINED</definition-type>
  <created-by-user-name>Juniper Networks Inc.</created-by-user-name>
  <id>32769</id>
  <destination-address-translation>NONE</destination-address-translation>
  <service-offload>>false</service-offload>
  <name>Log Session Close</name>
  <description>Predefined profile that logs at session close</description>
  <enable-count>>false</enable-count>
  <log-at-session-close>>true</log-at-session-close>
  <log-at-session-init-time>>false</log-at-session-init-time>
  <redirect>NONE</redirect>
  <authentication-type>NONE</authentication-type>
  <infranet-redirect>NONE</infranet-redirect>
  <default-profile>>false</default-profile>
  <sd-template/>
  <tcp-syn-check>>false</tcp-syn-check>
  <tcp-seq-check>>false</tcp-seq-check>
</policy-profile>
```

### Sample Policy Profile Management Input and Output with Pagination

URI	Description
/api/juniper/sd/fwpolicy-management/policy-profiles?paging=(limit eq 10)	Ten policy profiles are listed.
/api/juniper/sd/fwpolicy-management/policy-profiles?paging=(start eq 10 limit eq 5)	From the record number 10, five policy profiles are listed.

### Sample Policy Profile Management Input and Output with Filtering

URI: /api/juniper/sd/fwpolicy-management/policy-profiles?filter=(name eq 'Log Session Init')

This policy search is similar to the left pane search of the Security Director policy page.

### Sample Policy Profile Management Input and Output With Sorting

URI	Description
/api/juniper/sd/fwpolicy-management/policy-profiles?sortby=(name(ascending))	All policy profile names are sorted in an ascending order.
/api/juniper/sd/fwpolicy-management/policy-profiles?sortby=(name(descending))	All policy profile names are sorted in an ascending order.

## POST

This request is used to create a new policy profile

URI	/api/juniper/sd/fwpolicy-management/policy-profiles
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.fwpolicy-management.policy-profile+xml;version="1" application/vnd.juniper.sd.fwpolicy-management.policy-profile+JSON;version=1;q=0.01
Consumes	None
Produces	Create a new policy profile

#### Sample XML Input

```
<policy-profile>
  <name>policyProfile-1_auth1</name>
  <edit-version>0</edit-version>
  <definition-type>CUSTOM</definition-type>
  <created-by-user-name>super</created-by-user-name>
  <last-modified-by-user-name />
  <id />
  <destination-address-translation>NONE
</destination-address-translation>
```

```

<service-offload>>false</service-offload>
<description>Deny all and log start of incidents</description>
<enable-count>>true</enable-count>
<per-minute-alarm-threshold>20</per-minute-alarm-threshold>
<per-second-alarm-threshold>5</per-second-alarm-threshold>
<log-at-session-close>>false</log-at-session-close>
<log-at-session-init-time>true</log-at-session-init-time>
<redirect>NONE</redirect>
<authentication-type>NONE</authentication-type>
<redirect-url />
<infranet-redirect>NONE</infranet-redirect>
<default-profile>>false</default-profile>
<tcp-syn-check>>false</tcp-syn-check>
<tcp-seq-check>>false</tcp-seq-check>
</policy-profile>

```

## PUT

This request is used to modify a policy profile.

URI	/api/juniper/sd/fwpolicy-management/policy-profiles/{profile-id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.fwpolicy-management.policy-profile+xml;version="1" application/vnd.juniper.sd.fwpolicy-management.policy-profile+JSON;version=1;q=0.01
Consumes	None
Produces	Modifies a policy profile

### Sample XML Modified Value

```

<policy-profile>
  <name>policyProfile-1_auth1</name>
  <edit-version>1</edit-version>
  <definition-type>CUSTOM</definition-type>
  <created-by-user-name>super</created-by-user-name>
  <last-modified-by-user-name />
  <id>327789</id>
  <destination-address-translation>NONE
</destination-address-translation>
  <service-offload>>false</service-offload>
  <description>Deny all and log start of incidents</description>
  <enable-count>>true</enable-count>
  <per-minute-alarm-threshold>20</per-minute-alarm-threshold>
  <per-second-alarm-threshold>5</per-second-alarm-threshold>
  <log-at-session-close>>false</log-at-session-close>
  <log-at-session-init-time>true</log-at-session-init-time>
  <redirect>NONE</redirect>
  <authentication-type>NONE</authentication-type>
  <redirect-url />
  <infranet-redirect>NONE</infranet-redirect>
  <default-profile>>false</default-profile>
  <tcp-syn-check>>false</tcp-syn-check>

```

```
<tcp-seq-check>false</tcp-seq-check>
</policy-profile>
```

DELETE

This request is used to delete a policy profile.

URI	/api/juniper/sd/fwpolicy-management/policy-profiles/{profile-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.fwpolicy-management.policy-profile+xml;version="1" application/vnd.juniper.sd.fwpolicy-management.policy-profile+JSON;version=1;q=0.01
Consumes	None
Produces	Delete a policy profile

PATCH

This request is used to patch or make a partial update to the policy profile.

URI	/api/juniper/sd/fwpolicy-management/policy-profiles/{profile-id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.fwpolicy-management.policy-profile_patch+json;version=1;charset=UTF-8
Consumes	None
Produces	Patches a policy profile

**Sample XML Input**

```
<diff>
  <replace sel=policy-profile/name>
    <name>policyProfile-1_patch</name>
  </replace>
</diff>
```

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)



CHAPTER 11

# VPN Management RESTful Web Services

- [VPN Management RESTful Web Services on page 129](#)

## VPN Management RESTful Web Services

The following operations can be performed using the Security Director VPN Management RESTful Web Services.

### IPsec VPN

#### GET

This request is used to collect all the IPsec VPNs.

URI	/api/juniper/sd/vpn-management
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.vpn-management.ipsec-vpns+xml;version="1" application/vnd.juniper.sd.vpn-management.ipsec-vpns+json;version="1"
Consumes	None
Produces	Links to manage IPsec VPN, Extranet, VPN Profile and Publish VPN

#### Sample VPN Management output

##### Sample XML Output

```
<vpn-management>
  <collection href="/api/juniper/sd/vpn-management/ipsec-vpns" rel="ipsec-vpns"/>

  <collection href="/api/juniper/sd/vpn-management/extranet-devices"
rel="extranet-devices"/>
  <collection href="/api/juniper/sd/vpn-management/vpn-profiles" rel="vpn-profiles"/>

  <method href="/api/juniper/sd/vpn-management/publish" rel="publish"/>
</vpn-management>
```

#### Sample VPN Management Input and Output to Get All VPNs

URI: /api/juniper/sd/vpn-management/ipsec-vpns

**Sample XML Output**

```
<ipsec-vpns total="1" uri="/api/juniper/sd/vpn-management/ipsec-vpns">
  <ipsec-vpn href="/api/juniper/sd/vpn-management/ipsec-vpns/623018"
uri="/api/juniper/sd/vpn-management/ipsec-vpns/623018">
    <id>623018</id>
    <edit-version>1</edit-version>
    <name>vpn-ss</name>
    <unique-key-per-tunnel>true</unique-key-per-tunnel>
    <preshared-key-type>AUTO_GENERATE</preshared-key-type>
    <publish-state>NOT_PUBLISHED</publish-state>
    <type>SITE_TO_SITE</type>
    <vpn-tunnel-mode-types>ROUTE_BASED</vpn-tunnel-mode-types>
    <profile href="/api/juniper/sd/vpn-management/vpn-profiles/65536">
      <name>MainModeProfile</name>
      <id>65536</id>
    </profile>
    <description>
    </description>
  </ipsec-vpn>
</ipsec-vpns>
```

**Sample VPN Management Input and Output to Get VPN by ID**

URI: /api/juniper/sd/vpn-management/ipsec-vpns/623018

This request is used to get a VPN by its ID. The request returns the VPN information such as name, description, tunnel-mode, vpn-type, vpn-profile, preshared-key, tunnel-settings, and route-settings. It also includes two hrefs, one pointing to all the devices that are part of the VPN, and the other pointing to all the tunnels that are part of the VPN. The API also returns the edit version of the VPN which must be used when you modify thi particular VPN to safe guard from the concurrent modification related issues.

**Sample XML Output**

```
<ipsec-vpn uri="/api/juniper/sd/vpn-management/ipsec-vpns/98312">
  <edit-version>5</edit-version>
  <version>5</version>
  <created-by-user-name>super</created-by-user-name>
  <last-modified-by-user-name>super</last-modified-by-user-name>
  <domain-id>2</domain-id>
  <id>98312</id>
  <name>HnS_Rest_VPN_1</name>
  <description/>
  <profile href= "/api/juniper/sd/vpn-management/vpn-profiles/98304" >
    <name>MainModeProfile</name>
    <id>98304</id>
  </profile>
  <vpn-tunnel-mode-types>ROUTE_BASED</vpn-tunnel-mode-types>
  <type>HUB_N_SPOKE</type>
  <tunnel-interface-type>UNNUMBERED</tunnel-interface-type>
  <tunnel-ip-range>
  <mask>0</mask>
  </tunnel-ip-range>
  <tunnel-multi-point-size>1</tunnel-multi-point-size>
  <publish-state>NOT_PUBLISHED</publish-state>
  <routing-type>STATIC</routing-type>
  <preshared-key-type>AUTO_GENERATE</preshared-key-type>
  <unique-key-per-tunnel>true</unique-key-per-tunnel>
  <ospf-area-id>0</ospf-area-id>
```



```

<max-retrans-time>0</max-retrans-time>
<policy-state>FINAL</policy-state>
<allow-spoke-to-spoke-communication>>false</allow-spoke-to-spoke-communication>
<auto-vpn>>false</auto-vpn>
<multi-proxyid>>false</multi-proxyid>
<domain-name>Global</domain-name>
<devices href= "/api/juniper/sd/vpn-management/ipsec-vpns/98312/devices" />
<tunnels href= "/api/juniper/sd/vpn-management/ipsec-vpns/98312/tunnels" />
</ipsec-vpn>

```

### Sample VPN Management Input and Output to Get All Devices of VPN

URI: /api/juniper/sd/vpn-management/ipsec-vpns/623018/devices

This request is used to get all the devices participating in a VPN and details related to that device such as the device name, whether the device is a hub or spoke, protected-networks, external-interface, proxy-id, and so on. This API supports paging and filtering. It supports global search for filtering by device name and device IP.

#### Sample XML Output

```

<devices total="2" uri="/api/juniper/sd/vpn-management/ipsec-vpns/623018/devices">

  <device>
    <certificate>
    </certificate>
    <is-hub>>false</is-hub>
    <initiator>>false</initiator>
    <external-if-name>ge-0/0/3.0</external-if-name>
    <proxy-id>
    </proxy-id>
    <protected-networks total="0"/>
    <protected-network-zones total="1">
      <protected-network-zone>trust</protected-network-zone>
    </protected-network-zones>
    <tunnel-zone>zone1</tunnel-zone>
    <export-default-routes>>false</export-default-routes>
    <export-static-routes>>false</export-static-routes>
    <export-ospf-routes>>false</export-ospf-routes>
    <export-rip-routes>>false</export-rip-routes>
    <metric>-1</metric>
    <extranet-device>>false</extranet-device>
    <tunnel-vr>VR_1</tunnel-vr>
    <device-moid>net.juniper.jnap.sm.om.jpaa.SecurityDeviceEntity:65561</device-moid>

    <device-name>sd-srx240-1</device-name>
    <device-ip>10.205.119.5</device-ip>
    <edit-version>0</edit-version>
    <version>0</version>
  </device>
  <device>
    <certificate>
    </certificate>
    <is-hub>>false</is-hub>
    <initiator>>false</initiator>
    <external-if-name>ge-0/0/7.0</external-if-name>
    <proxy-id>10.1.20.1/32</proxy-id>
    <protected-networks total="0"/>

```

```

<protected-network-zones total="1">
<protected-network-zone>trust</protected-network-zone>
</protected-network-zones>
<tunnel-zone>zone1</tunnel-zone>
<export-default-routes>>false</export-default-routes>
<export-static-routes>>false</export-static-routes>
<export-ospf-routes>>false</export-ospf-routes>
<export-rip-routes>>false</export-rip-routes>
<metric>-1</metric>
<extranet-device>>false</extranet-device>
<tunnel-vr>
</tunnel-vr>
<device-moid>net.juniper.jnap.sm.om.jp.a.SecurityDeviceEntity:65558</device-moid>

<device-name>10.205.50.210</device-name>
<device-ip>10.205.50.210</device-ip>
<edit-version>0</edit-version>
<version>0</version>
</device>
</devices>

```

### Sample VPN Management Input and Output to Get All Tunnels of VPN

URI: /api/juniper/sd/vpn-management/ipsec-vpns/623018/tunnels

This request is used to get all the tunnels of a VPN. The details include peer device, VPN name, VPN profile, IKE ID, preshared key, external interface, tunnel interface and tunnel zone. It support global search for searching on device name or device IP.

#### Sample XML Output

```

<tunnels uri="/api/juniper/sd/vpn-management/ipsec-vpns/98312/tunnels" total="2">
<tunnel>
<device-name>sd-srx240-2</device-name>
<external-if-name>ge-0/0/1.0</external-if-name>
<tunnel-zone/>
<peer-device>
<device-name>sd-srx650-4</device-name>
<device-ip>10.207.97.137</device-ip>
</peer-device>
<traffic-selectors/>
<tunnel-if-name>st0.1</tunnel-if-name>
<ike-id>198.51.100.1</ike-id>
<vpn-name-in-device>sd-srx650-4_HnS_Rest_VPN_1</vpn-name-in-device>
<local-proxyid>192.0.2.1</local-proxyid>
<remote-proxyid>192.0.2.2</remote-proxyid>
<ike-gateway-name>sd-srx650-4_HnS_Rest_VPN_1</ike-gateway-name>
<ike-policy-name>sd-srx650-4_HnS_Rest_VPN_1</ike-policy-name>
<ipsec-policy-name>HnS_Rest_VPN_1</ipsec-policy-name>
<preshared-key>
$ABC123
</preshared-key>
<profile/>
<device-ip>10.207.97.139</device-ip>
<edit-version>0</edit-version>
<version>0</version>
<domain-id>2</domain-id>
<id>98315</id>

```

```

</tunnel>
<tunnel>
<device-name>sd-srx650-4</device-name>
<external-if-name>ge-0/0/1.0</external-if-name>
<tunnel-zone/>
<peer-device>
<device-name>sd-srx240-2</device-name>
<device-ip>10.207.97.139</device-ip>
</peer-device>
<traffic-selectors/>
<tunnel-if-name>st0.1</tunnel-if-name>
<ike-id>198.51.100.1</ike-id>
<vpn-name-in-device>sd-srx240-2_HnS_Rest_VPN_1</vpn-name-in-device>
<local-proxyid>192.0.2.3</local-proxyid>
<remote-proxyid>192.0.2.4</remote-proxyid>
<ike-gateway-name>sd-srx240-2_HnS_Rest_VPN_1</ike-gateway-name>
<ike-policy-name>sd-srx240-2_HnS_Rest_VPN_1</ike-policy-name>
<ipsec-policy-name>HnS_Rest_VPN_1</ipsec-policy-name>
<preshared-key>
$ABC123
</preshared-key>
<profile/>
<device-ip>10.207.97.137</device-ip>
<edit-version>0</edit-version>
<version>0</version>
<domain-id>2</domain-id>
<id>98317</id>
</tunnel>
</tunnels>

```

### Sample VPN Management Input and Output with Pagination

URI	Description
/api/juniper/sd/vpn-management/ipsec-vpns?paging=(limit eq 4)	The first four VPNs in the first page are listed.
/api/juniper/sd/vpn-management/ipsec-vpns?paging=(start eq 2, limit eq 4)	From the record 3, two VPNs are listed

### Sample VPN Management Input and Output with Filtering

URI: /api/juniper/sd/vpn-management/ipsec-vpns?filter=(global eq 'HnS\_Key')

All VPN names matching with *HnS-Key* are filtered and listed.

#### Sample XML Output

```

<ipsec-vpns total="2" uri="/api/juniper/sd/vpn-management/ipsec-vpns">
  <ipsec-vpn href="/api/juniper/sd/vpn-management/ipsec-vpns/32802"
uri="/api/juniper/sd/vpn-management/ipsec-vpns/32802">
    <id>32802</id>
    <edit-version>7</edit-version>
    <name>HnS_Key</name>
    <unique-key-per-tunnel>true</unique-key-per-tunnel>
    <preshared-key-type>AUTO_GENERATE</preshared-key-type>
    <publish-state>FULLY_PUBLISHED</publish-state>
    <type>HUB_N_SPOKE</type>

```

```

    <vpn-tunnel-mode-types>ROUTE_BASED</vpn-tunnel-mode-types>
    <profile href="/api/juniper/sd/vpn-management/vpn-profiles/32815">
      <name>CustomMainPre</name>
      <id>32815</id>
    </profile>
    <description>
    </description>
  </ipsec-vpn>
</ipsec-vpns>

```

URI: /api/juniper/sd/vpn-management/ipsec-vpns?filter=(global eq 'HnS\_Key or CC\_Mesh' )

All VPN names matching with *HnS-Key* or *CC-Mesh* are filtered and listed.

## POST

This request is used to create a new IPsec VPN. The API requires the information such as - VPN name, tunnel mode, VPN type, VPN profile, preshared key, tunnel settings, route settings, and devices that are part of the VPN and device setting details per device such as if the device is hub or spoke, external interface of the device, tunnel zone, protected networks of the device, and route settings.

URI	/api/juniper/sd/vpn-management/ipsec-vpns/create-vpn
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.vpn-management.ipsec-vpns.create-vpn+xml;version=2;charset=UTF-8 application/vnd.juniper.sd.vpn-management.ipsec-vpns.create-vpn+json;version=2;charset=UTF-8
Consumes	None
Produces	Creates a new IPsec VPN

To create a new IPsec VPN, send the VPN information, as shown in the following example. Copy this information in the Body window, and send it to the Junos Space server.

### Sample XML Input

```

<create-vpn>
  <vpn-mo>
    <name>HnS_RestVPN</name>
    <max-retrans-time>0</max-retrans-time>
    <ospf-area-id>0</ospf-area-id>
    <unique-key-per-tunnel>true</unique-key-per-tunnel>
    <preshared-key-type>AUTO_GENERATE</preshared-key-type>
    <routing-type>STATIC</routing-type>
    <tunnel-multi-point-size>-1</tunnel-multi-point-size>
    <tunnel-interface-type>UNNUMBERED</tunnel-interface-type>
    <type>HUB_N_SPOKE</type>
    <vpn-tunnel-mode-types>ROUTE_BASED</vpn-tunnel-mode-types>
  </profile>
  <name>MainModeProfile</name>
  <id>65536</id>
</profile>

```

```

    <description>Created through REST API</description>
  </vpn-mo>
  <devices>
    <vpn-device-bean>
      <is-hub>true</is-hub>
      <external-if-name>reth1.0</external-if-name>
      <proxy-id>192.0.2.0/24</proxy-id>
      <tunnel-zone>VPN</tunnel-zone>
      <protected-network-zones total="0">
        <protected-network-zon>trust</protected-network-zon>
      </protected-network-zones>
      <extranet-device>>false</extranet-device>
      <tunnel-vr>
      </tunnel-vr>
      <device-name>Node-177-178-cluster-logical-system1</device-name>
      <device-moid>net.juniper.jnap.sm.om.jp.a.SecurityDeviceEntity:131080</device-moid>

    </vpn-device-bean>
    <vpn-device-bean>
      <is-hub>>false</is-hub>
      <external-if-name>reth0.0</external-if-name>
      <proxy-id>1.3.1.0/24</proxy-id>
      <tunnel-zone>VPN</tunnel-zone>
      <protected-networks total="0">
        <protected-network>
          <id>983510</id>
          <name>VPN_AD1</name>
        </protected-network>
        <protected-network>
          <id>983511</id>
          <name>VPN_AD2</name>
        </protected-network>
      </protected-networks>
      <extranet-device>>false</extranet-device>
      <tunnel-vr>
      </tunnel-vr>
      <device-name>10.205.119.19</device-name>
      <device-moid>net.juniper.jnap.sm.om.jp.a.SecurityDeviceEntity:131357</device-moid>

    </vpn-device-bean>
  </devices>
</create-vpn>

```

<max-retrans-time/> parameter is required for only RIP protocol and it is not a mandatory field.

<ospf-area-id/> is required only for OSPF protocol and it is not a mandatory field.

<tunnel-multi-point-size/> is used to control the number of peer devices that a tunnel interface can share. If the value is -1, single tunnel is shared for all the remote peers. For unnumbered tunnel interface type, tunnel sharing is not possible and the value should be set as 1 for all VPN types. If tunnel interface type is numbered, it must be set as -1 for site-to-site and full-mesh VPNs, for hub & spoke VPNs it can be -1 or any positive value.

**Modify VPN**

This request is used to modify an existing IPsec VPN. The API requires the information such as VPN name, tunnel mode, VPN type, VPN profile, preshared key, tunnel settings, route settings, devices that are part of the VPN and device setting details per device such as if the device is hub or spoke, external interface of the device, tunnel zone, protected networks of the device, and route settings. You must provide the edit version to safeguard from concurrent modification related issues.

URI: /api/juniper/sd/vpn-management/ipsec-vpns/modify-vpn

Content-Type:

application/vnd.junipersd.vpn-management.ipsec-vpns.modify-vpn+xml;version=2; charset=UTF-8

**Sample XML Input**

```
<modify-vpn>
  <vpn-mo>
    <id>1769488</id>
    <version>0</version>
    <edit-version>0</edit-version>
    <name>S2S_RestVPN</name>
    <unique-key-per-tunnel>true</unique-key-per-tunnel>
    <preshared-key-type>AUTO_GENERATE</preshared-key-type>
    <routing-type>STATIC</routing-type>
    <tunnel-multi-point-size>-1</tunnel-multi-point-size>
    <tunnel-ip-range>
      <mask>24</mask>
      <network-ip>1.2.3.0</network-ip>
    </tunnel-ip-range>
    <tunnel-interface-type>NUMBERED</tunnel-interface-type>
    <type>SITE_TO_SITE</type>
    <vpn-tunnel-mode-types>ROUTE_BASED</vpn-tunnel-mode-types>
    <profile>
      <name>MainModeProfile</name>
      <id>65536</id>
    </profile>
    <description>Modified through REST API</description>
  </vpn-mo>
  <device-modification>
    <devices-to-add>
      <vpn-device-bean>
        <is-hub>>false</is-hub>
        <external-if-name>ge-0/0/1.0</external-if-name>
        <tunnel-zone>VPN</tunnel-zone>
        <protected-network-zones total="0">
          <protected-network-zon>trust</protected-network-zon>
        </protected-network-zones>
        <export-default-routes>>false</export-default-routes>
        <export-static-routes>>false</export-static-routes>
        <export-ospf-routes>>false</export-ospf-routes>
        <export-rip-routes>>false</export-rip-routes>
        <metric>0</metric>
        <extranet-device>>false</extranet-device>
        <device-name>sd-srx240-1</device-name>
        <device-moid>net.juniper.jmp.jp.a.SecurityDeviceEntity:1343512</device-moid>
      </vpn-device-bean>
    </devices-to-add>
  </device-modification>
</modify-vpn>
```

```

</devices-to-add>
<device-mo-ids-to-delete>

<device-mo-ids-to-delet>net.juniper.jmp.jpa.SecurityDeviceEntity:2162696</device-mo-ids-to-delet>

</device-mo-ids-to-delete>
<devices-to-modify>
<vpn-device-bean>
<is-hub>>false</is-hub>
<external-if-name>ge-0/0/3.0</external-if-name>
<tunnel-zone>modtest</tunnel-zone>
<protected-networks total="0">
<protected-network>
<id>983510</id>
<name>VPN_AD1</name>
</protected-network>
<protected-network>
<id>983511</id>
<name>VPN_AD2</name>
</protected-network>
</protected-networks>
<export-default-routes>>false</export-default-routes>
<export-static-routes>>false</export-static-routes>
<export-ospf-routes>>false</export-ospf-routes>
<export-rip-routes>>false</export-rip-routes>
<extranet-device>>false</extranet-device>
<device-name>sd-srx240-2</device-name>
<device-moid>net.juniper.jmp.jpa.SecurityDeviceEntity:1343504</device-moid>
</vpn-device-bean>
</devices-to-modify>
</device-modification>
</modify-vpn>

```

The following mandatory fields are required to modify a VPN:

- ID
- Edit version
- VPN type must be same (it cannot be modified)
- TunnelModeType must be same (it cannot be modified)

### **Modify Tunnels**

This request is used to modify VPN tunnels in bulk. This API expects list of modified tunnels. Each member of this list is a modified tunnel. The tunnel related parameters such as VPN name, IKE ID and Preshared key can be modified.

URI: /api/juniper/sd/vpn-management/ipsec-vpns/modify-tunnels

Content-Type:

application/vnd.juniper.sd.vpn-management.ipsec-vpns.modify-tunnels+xml;version=2; charset=UTF-8

#### **Sample XML Input to Modify a Tunnel**

```

<modify-tunnels>
<vpn-basic>
<id>98312</id>

```

```
<edit-version>11</edit-version>
<name>HnS_RestVPN_1</name>
</vpn-basic>

<end-points>
<vpn-end-point>
<device-name>sd-srx240-2</device-name>
<external-if-name>ge-0/0/1.0</external-if-name>
<tunnel-zone/>
<peer-device>
<device-name>sd-srx650-4</device-name>
<device-ip>10.207.97.137</device-ip>
</peer-device>
<local-proxyid>192.0.2.6</local-proxyid>
<remote-proxyid>192.0.2.7</remote-proxyid>
<ike-id>198.51.100.5</ike-id>
<vpn-name-in-device>sd-srx650-4_HnS_Rest_change</vpn-name-in-device>
<ike-gateway-name>sd-srx650-4_HnS_Rest_change</ike-gateway-name>
<ike-policy-name>sd-srx650-4_HnS_Rest_change</ike-policy-name>
<ipsec-policy-name>HnS_Rest_VPN_1</ipsec-policy-name>
<profile/>
<device-ip>10.207.97.139</device-ip>
<edit-version>0</edit-version>
<id>98315</id>
</vpn-end-point>
</end-points>
</modify-tunnels>

<modify-tunnels>
<vpn-basic>
<id>98321</id>
<edit-version>19</edit-version>
<name>HnS_MPID_VPN</name>
</vpn-basic>

<end-points>
<vpn-end-point>
<traffic-selectors>
<traffic-selector>
<local-ip>192.0.2.3</local-ip>
<remote-ip>192.0.2.4</remote-ip>
<name>Traffic_Selector_2</name>
</traffic-selector>
</traffic-selectors>
<tunnel-if-name>st0.1</tunnel-if-name>
<ike-id>198.51.100.1</ike-id>
<vpn-name-in-device/>
<local-proxyid/>
<remote-proxyid/>
<ike-gateway-name>sd-srx650-4_HnS_MPID_VPN</ike-gateway-name>
<ike-policy-name>sd-srx650-4_HnS_MPID_VPN</ike-policy-name>
<ipsec-policy-name>HnS_MPID_VPN</ipsec-policy-name>
<device-ip>10.207.97.139</device-ip>
<edit-version>0</edit-version>
<id>98326</id>
```



```

</vpn-end-point>
</end-points>
</modify-tunnels>

```

The following mandatory fields are required to modify a tunnel:

- VPN ID
- VPN edit version
- Tunnel ID

### **Publish VPN**

This request is used to schedule a job and publish a VPN. After the publish, you must use the device update RESTful Web Services to update the devices.

URI	api/juniper/sd/vpn-management/publish
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.vpn-management.publish+xml;version=1;charset=UTF-8"
Consumes	None
Produces	Publishes the IPsec VPN

Send the publish information to the Junos Space server, as shown in the following example.

#### **Sample XML Input**

```

<publish>
  <vpn-ids>
    <vpn-id>Integer</vpn-id>
  </vpn-ids>
</publish>

```

### **Sample VPN Management Input for Scheduling of Publish Operation**

URI: /api/juniper/sd/vpn-management/publish?schedule=(at(01 01 11 26 05 ? 2013))

The syntax for scheduling a publish at a particular time is schedule= (at(ss mm HH dd MM ? yy)).

- ss—Seconds (mandatory field)
- mm—Minutes (mandatory field)
- HH—Hours (mandatory field)
- dd—Day of the month (mandatory field)
- EE—Day of week (mandatory field)
- MM—Month (mandatory field)

- yy—Year (optional field)
- ?—This is the allowed value of EE.

If you want to schedule the update after a particular time, send the information as shown in the following example.

URI: /api/juniper/sd/ vpn-management/publish?schedule=(after(00 00 30))

The syntax for scheduling after a particular time period is schedule=(after(dd HH mm)) or schedule=(after(HH mm)).

- dd—Days (optional parameter)
- HH—Hours
- mm—Minutes

## DELETE

This request is used to delete a VPN.

URI	/api/juniper/sd/vpn-management/ipsec-vpns/{vpn-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.vpn-management.delete+xml;version=1;charset=UTF-8"
Consumes	None
Produces	Deletes a VPN

## Extranet Devices

### GET

This request is used to get all extranet devices. Get all extranet-devices support paging, sorting by name and global filtering.

URI	/api/juniper/sd/vpn-management/extranet-devices
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.vpn-management.extranet-devices+xml;q=0.01;version=1
Consumes	None
Produces	Collection of extranet devices

### Sample VPN Management Input and Output to Get All Extranet Devices

**Sample XML Output**      <extranet-devices total="3" uri="/api/juniper/sd/vpn-management/extranet-devices">

```

    <extranet-device href="/api/juniper/sd/vpn-management/extranet-devices/524714"
uri="/api/juniper/sd/vpn-management/extranet-devices/524714">
    <name>ExtranetDevice1</name>
    <description>Created by backend automation</description>
    <ip-address>192.0.2.10</ip-address>
    <host-name>ExtranetDevice1</host-name>
    <id>524714</id>
</extranet-device>
<extranet-device href="/api/juniper/sd/vpn-management/extranet-devices/524715"
uri="/api/juniper/sd/vpn-management/extranet-devices/524715">
    <name>ExtranetDevice2</name>
    <description>Created by backend automation</description>
    <ip-address>192.0.2.11</ip-address>
    <host-name>ExtranetDevice2</host-name>
    <id>524715</id>
</extranet-device>
<extranet-device href="/api/juniper/sd/vpn-management/extranet-devices/524716"
uri="/api/juniper/sd/vpn-management/extranet-devices/524716">
    <name>ExtranetDevice3</name>
    <description>Created by backend automation</description>
    <ip-address>192.0.2.12</ip-address>
    <host-name>ExtranetDevice3</host-name>
    <id>524716</id>
</extranet-device>
</extranet-devices>

```

### Sample VPN Management Input and Output to Get Extranet Device By ID

URI: /api/juniper/sd/vpn-management/extranet-devices/524714

This request is used to get an extranet device by its ID. This request returns the information such as name, definition type, edit version, host name, IP address, description, and ID. The edit version of the extranet device must be used when you modify this particular extranet device to safeguard from the concurrent modification related issues.

#### Sample XML Output

```

<extranet-device uri="/api/juniper/sd/vpn-management/extranet-devices/524714">
  <name>ExtranetDevice1</name>
  <definition-type>CUSTOM</definition-type>
  <edit-version>0</edit-version>
  <host-name>ExtranetDevice1</host-name>
  <ip-address>192.0.2.13</ip-address>
  <description>Created by backend automation</description>
  <id>524714</id>
</extranet-device>

```

### POST

This request is used to create an extranet device.

URI	/api/juniper/sd/vpn-management/extranet-devices
HTTP Method	HTTP POST

Content-Type	application/vnd.juniper.sd.vpn-management.extranet-device+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.vpn-management.extranet-device+json;version=1;charset=UTF-8
Consumes	None
Produces	Creates a new extranet device

To create a new extranet device, send the new extranet device information to the Junos Space server, as shown in the following example.

#### Sample XML Input

```
<extranet-device>
  <name>ext_REST_device</name>
  <created-by-user-name>super</created-by-user-name>
  <host-name>kk</host-name>
  <ip-address>10.207.96.88</ip-address>
  <description>created from REST</description>
</extranet-device>
<extranet-device>
  <name>ext_REST_device_2</name>
  <created-by-user-name></created-by-user-name>
  <host-name>host2</host-name>
  <ip-address></ip-address>
  <description>created from REST 2</description>
</extranet-device>
<extranet-device>
  <name>ext_REST_device_3</name>
  <created-by-user-name></created-by-user-name>
  <host-name></host-name>
  <ip-address>192.0.2.3</ip-address>
  <description></description>
</extranet-device>
```

## PUT

This request is used to modify an extranet device.

URI	/api/juniper/sd/vpn-management/extranet-devices/{extranet-device-id}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.vpn-management.extranet-device+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.vpn-management.extranet-device+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies an extranet device

To modify an extranet device, send the edit information to the Junos Space server, as shown in the following example.

**Sample XML Input**

```
<extranet-device>
  <name>ext_REST_device</name>
  <created-by-user-name>Super</created-by-user-name>
  <definition-type>HIDDEN</definition-type>
  <edit-version>0</edit-version>
  <host-name>kaykay</host-name>
  <ip-address>10.207.96.99</ip-address>
  <description>changed from REST</description>
  <id>7634944</id>
</extranet-device>
```

**PATCH**

This request is used to patch or to make partial updates to an extranet device.

URI	/api/juniper/sd/vpn-management/extranet-devices/{extranet-device-id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.vpn-management.extranet-device_patch+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.vpn-management.extranet-device_patch+json;version=1;charset=UTF-8
Consumes	None
Produces	Patches an extranet device

To patch an extranet device, send the patch information to the Junos Space server, as shown in the following example.

**Sample XML Input for Name**

```
<diff>
  <replace sel="extranet-device/description">
    <description>This is patched</description>
  </replace>
</diff>
```

**Sample XML Input for Host**

```
<diff>
  <replace sel=extranet-device/host-name>
    <host-name>www.live.in</host-name>
  </replace>
</diff>
```

**Sample XML Input for IP Address**

```
<diff>
  <replace sel=extranet-device/ip-address>
    <ip-address>192.0.2.2</ip-address>
  </replace>
  <replace sel=extranet-device/description>
    <description>description patched again</description>
  </replace>
</diff>
```

**Sample XML Input for Empty IP Address**

```
<diff>
  <replace sel=extranet-device/ip-address>
    <ip-address></ip-address>
```

```

</replace>
<replace sel=extranet-device/host-name>
  <host-name>emptyIP</host-name>
</replace>
</diff>

```

## DELETE

This request is used to delete an extranet device.

URI	/api/juniper/sd/vpn-management/extranet-devices/{extranet-device-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.vpn-management.extranet-devices+xml;q=0.01;version=1
Consumes	None
Produces	Deletes an extranet device

## VPN Profiles

### GET

This request is used to get all vpn profiles. Get all vpn profiles support paging, sorting by name and global filtering.

URI	/api/juniper/sd/vpn-management/vpn-profiles
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.vpn-management.vpn-profiles+xml;version=1;q=0.01 application/vnd.juniper.sd.vpn-management.vpn-profiles+json;version=1;q=0.01
Consumes	None
Produces	Collection of VPN profiles

### Sample VPN Management Input and Output to Get All VPN Profiles

#### Sample XML Output

```

<vpn-profiles total="2" uri="/api/juniper/sd/vpn-management/vpn-profiles">
  <vpn-profile href="/api/juniper/sd/vpn-management/vpn-profiles/65536"
uri="/api/juniper/sd/vpn-management/vpn-profiles/65536">
    <name>MainModeProfile</name>
    <description>Predefined Main mode profile with Standard proposal set</description>

    <definition-type>PREDEFINED</definition-type>
    <id>65536</id>
  </vpn-profile>
  <vpn-profile href="/api/juniper/sd/vpn-management/vpn-profiles/65537"
uri="/api/juniper/sd/vpn-management/vpn-profiles/65537">
    <name>AggressiveModeProfile</name>

```

```

    <description>Predefined Aggressive mode profile with Standard proposal
set</description>
    <definition-type>PREDEFINED</definition-type>
    <id>65537</id>
  </vpn-profile>
</vpn-profiles>

```

### Sample VPN Management Input and Output to Get VPN Profile by ID

URI: /api/juniper/sd/vpn-management/vpn-profiles/65536

This request is used to get a VPN profile by its ID.

#### Sample XML Output

```

<vpn-profile uri="/api/juniper/sd/vpn-management/vpn-profiles/98318">
  <name>VPN_Profile_REST_1</name>
  <last-modified-by-user-name>super</last-modified-by-user-name>
  <created-by-user-name>super</created-by-user-name>
  <phase2-setting>
    <phase2-proposal-type>CUSTOM</phase2-proposal-type>
    <custom-phase2-proposals>
      <phase2-proposal>
        <name>Custom-proposal-1</name>
        <protocol>esp</protocol>
        <authentication-algorithm>sha_1</authentication-algorithm>
        <encryption-algorithm>aes_cbc_128</encryption-algorithm>
        <lifetime>3602</lifetime>
        <life-size>66</life-size>
        <moid>
          net.juniper.space.sd.vpnmanager.jpa.Phase2ProposalEntity:98319
        </moid>
        <edit-version>0</edit-version>
        <version>0</version>
        <definition-type>CUSTOM</definition-type>
        <id>98319</id>
      </phase2-proposal>
    </custom-phase2-proposals>
    <idle-time>0</idle-time>
    <install-time>0</install-time>
    <dfbit>NONE</dfbit>
    <enable-anti-replay>true</enable-anti-replay>
    <enable-vpn-monitor>true</enable-vpn-monitor>
    <enable-vpn-optimized>true</enable-vpn-optimized>
    <establish-tunnel-immediately>true</establish-tunnel-immediately>
    <pfs>group2</pfs>
  </phase2-setting>
  <phase1-setting>
    <mode>MAIN</mode>
    <ike-id>HOSTNAME</ike-id>
    <ike-version>DEFAULT</ike-version>
    <auth-method>PRESHARED_KEY</auth-method>
    <phase1-proposal-type>PREDEFINED</phase1-proposal-type>
    <phase1-predefined-proposal-set>Compatible</phase1-predefined-proposal-set>
    <custom-phase1-proposals/>
    <enable-nat-traversal>true</enable-nat-traversal>
    <nat-traversal-keep-alive>3</nat-traversal-keep-alive>
    <enable-dpd>true</enable-dpd>
  </phase1-setting>
</vpn-profile>

```

```

<always-send-dpd>false</always-send-dpd>
<dpd-interval>0</dpd-interval>
<dpd-threshold>0</dpd-threshold>
</phase1-setting>
<edit-version>1</edit-version>
<definition-type>CUSTOM</definition-type>
<description/>
<domain-id>2</domain-id>
<id>98318</id>
<domain-name>Global</domain-name>
</vpn-profile>

```

## POST

This request is used to create a VPN profile.

URI	/api/juniper/sd/vpn-management/vpn-profiles
HTTP Method	HTTP POST
Content-Type	application/vnd.juniper.sd.vpn-management.vpn-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.vpn-management.vpn-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Creates a new VPN profile

To create a new VPN profile, send the new VPN profile information to the device, as shown in the following example.

### Sample XML Input1

```

<vpn-profile>
  <name>VPN_Profile_REST_3</name>
  <phase2-setting>
    <phase2-proposal-type>CUSTOM</phase2-proposal-type>
    <custom-phase2-proposals>
      <phase2-proposal>
        <name>Custom-proposal-1</name>
        <protocol>esp</protocol>
        <authentication-algorithm>sha_1</authentication-algorithm>
        <encryption-algorithm>aes_cbc_128</encryption-algorithm>
        <lifetime>3602</lifetime>
        <life-size>66</life-size>
      </phase2-proposal>
    </custom-phase2-proposals>
    <idle-time>0</idle-time>
    <install-time>0</install-time>
    <dfbit>NONE</dfbit>
    <enable-anti-replay>true</enable-anti-replay>
    <enable-vpn-monitor>true</enable-vpn-monitor>
    <enable-vpn-optimized>true</enable-vpn-optimized>
    <establish-tunnel-immediately>true</establish-tunnel-immediately>
    <pfs>group2</pfs>
  </phase2-setting>
  <definition-type>CUSTOM</definition-type>
</vpn-profile>

```



```

</phase2-setting>
<phase1-setting>
<mode>MAIN</mode>
<ike-id>HOSTNAME</ike-id>
<ike-version>V1</ike-version>
<auth-method>EC_DSA_SIGNATURE_256</auth-method>
<phase1-proposal-type>PREDEFINED</phase1-proposal-type>
<phase1-predefined-proposal-set>suiteb_gcm_256</phase1-predefined-proposal-set>
<custom-phase1-proposals/>
<enable-nat-traversal>true</enable-nat-traversal>
<nat-traversal-keep-alive>3</nat-traversal-keep-alive>
<enable-dpd>true</enable-dpd>
<always-send-dpd>false</always-send-dpd>
<dpd-interval>0</dpd-interval>
<dpd-threshold>0</dpd-threshold>
</phase1-setting>
<definition-type>CUSTOM</definition-type>
<description/>

</vpn-profile>

```

**Sample XML Input 2**

```

<vpn-profile>
  <name>VPN_Profile_REST_2</name>
  <phase2-setting>
    <phase2-proposal-type>PREDEFINED</phase2-proposal-type>

    <phase2-predefined-proposal-set>suiteb_gcm_256</phase2-predefined-proposal-set>

    <custom-phase2-proposals/>
    <idle-time>62</idle-time>
    <install-time>4</install-time>
    <dfbit>NONE</dfbit>
    <enable-anti-replay>true</enable-anti-replay>
    <enable-vpn-monitor>true</enable-vpn-monitor>
    <enable-vpn-optimized>true</enable-vpn-optimized>
    <establish-tunnel-immediately>true</establish-tunnel-immediately>
    <pfs>group24</pfs>
  </phase2-setting>
  <phase1-setting>
    <mode>MAIN</mode>
    <ike-id>HOSTNAME</ike-id>
    <ike-version>DEFAULT</ike-version>
    <auth-method>PRESHARED_KEY</auth-method>
    <phase1-proposal-type>CUSTOM</phase1-proposal-type>
    <custom-phase1-proposals>
      <phase1-proposal>
        <name>Custom_proposal_1</name>
        <dh-group>group20</dh-group>
        <authentication-algorithm>sha2_256</authentication-algorithm>
        <encryption-algorithm>aes_cbc_192</encryption-algorithm>
        <lifetime>28801</lifetime>

      </phase1-proposal>
      <phase1-proposal>
        <name>Custom_proposal_2</name>
        <dh-group>group24</dh-group>

```

```

    <authentication-algorithm>sha3_384</authentication-algorithm>
    <encryption-algorithm>aes_cbc_192</encryption-algorithm>
    <lifetime>3000</lifetime>

    </phase1-proposal>
  </custom-phase1-proposals>
  <enable-nat-traversal>true</enable-nat-traversal>
  <nat-traversal-keep-alive>2</nat-traversal-keep-alive>
  <enable-dpd>true</enable-dpd>
  <always-send-dpd>true</always-send-dpd>
  <dpd-interval>11</dpd-interval>
  <dpd-threshold>3</dpd-threshold>
</phase1-setting>
<edit-version>1</edit-version>
<definition-type>CUSTOM</definition-type>
<description></description>
</vpn-profile>

```

## PUT

This request is used to modify the VPN profile.

URI	/api/juniper/sd/vpn-management/vpn-profiles/{vpnProfileID}
HTTP Method	HTTP PUT
Content-Type	application/vnd.juniper.sd.vpn-management.vpn-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.vpn-management.vpn-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Modifies the VPN profile

To modify the VPN profile, send the edit information to the Junos Space server, as shown in the following example.

### Sample XML Input

```

<vpn-profile>
  <name>VPN_PROFILE_CREATED_FROM_REST</name>
  <phase2-setting>
    <phase2-proposal-type>PREDEFINED</phase2-proposal-type>
    <phase2-predefined-proposal-set>Basic</phase2-predefined-proposal-set>
    <custom-phase2-proposals />
    <idle-time>60</idle-time>
    <install-time>1</install-time>
    <dfbit>NONE</dfbit>
    <enable-anti-replay>true</enable-anti-replay>
    <enable-vpn-monitor>false</enable-vpn-monitor>
    <establish-tunnel-immediately>false</establish-tunnel-immediately>
    <pfs>group1</pfs>
  </phase2-setting>
  <phase1-setting>
    <mode>MAIN</mode>
    <ike-id>NONE</ike-id>
  </phase1-setting>
</vpn-profile>

```

```

<auth-method>PRESHARED_KEY</auth-method>
<phase1-proposal-type>PREDEFINED</phase1-proposal-type>
<phase1-predefined-proposal-set>Basic</phase1-predefined-proposal-set>
<custom-phase1-proposals />
<enable-nat-traversal>true</enable-nat-traversal>
<nat-traversal-keep-alive>5</nat-traversal-keep-alive>
<enable-dpd>false</enable-dpd>
<always-send-dpd>false</always-send-dpd>
<dpd-interval>10</dpd-interval>
<dpd-threshold>5</dpd-threshold>
<username></username>
</phase1-setting>
<edit-version>0</edit-version>
<definition-type>CUSTOM</definition-type>
<description>created from REST</description>
<id>7471104</id>
</vpn-profile>

```

## PATCH

This request is used to patch or to make a partial update to the VPN profile.

URI	/api/juniper/sd/vpn-management/vpn-profiles/{profile-id}
HTTP Method	HTTP PATCH
Content-Type	application/vnd.juniper.sd.vpn-management.vpn-profile_patch+xml;version=1;charset=UTF-8
Consumes	None
Produces	Patches the VPN profile

To patch the VPN profile, send the patch information to the Junos Space server, as shown in the following example.

### Sample XML Input for Name

```

<diff>
  <replace sel="vpn-profile/description">
    <description>This is patched</description>
  </replace>
</diff>

```

### Sample XML Input for Mode

```

<diff>
  <replace sel=vpn-profile/phase1-setting/mode>
    <mode>MAIN</mode>
  </replace>
  <replace sel=vpn-profile/description>
    <description>description patched</description>
  </replace>
</diff>

```

### Sample XML Input for Changing and Adding

```

<diff>
  <replace sel=vpn-profile/phase2-setting/phase2-proposal-type>
    <phase2-proposal-type>CUSTOM</phase2-proposal-type>

```

**Phase 2 Custom Proposal**

```

</replace>
<add sel=vpn-profile/phase2-setting/custom-phase2-proposals>
  <phase2-proposal>
    <name>testCustom1</name>
    <protocol>esp</protocol>
    <authentication-algorithm>sha_1</authentication-algorithm>
    <encryption-algorithm>aes_cbc_128</encryption-algorithm>
    <lifetime>3600</lifetime>
    <life-size>66</life-size>
  </phase2-proposal>
</add>
</diff>

```

**Sample XML Input for Deleting Custom Proposal**

```

<diff>
  <remove
sel=vpn-profile/phase1-setting/custom-phase1-proposals/phase1-proposal[name='testCustom5']>

  </diff>

```

**DELETE**

This request is used to delete the VPN profile

URI	/api/juniper/sd/vpn-management/vpn-profiles/{profile-id}
HTTP Method	HTTP DELETE
Content-Type	application/vnd.juniper.sd.vpn-management.vpn-profile+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.vpn-management.vpn-profile+json;version=1;charset=UTF-8
Consumes	None
Produces	Deletes the VPN profile

**Related Documentation**

- [Security Director RESTful Web Services Overview on page 3](#)
- [Using Security Director RESTful Web Services on page 5](#)

## PART 4

# Security Device Management

- [Device Management RESTful Web Services on page 153](#)



## CHAPTER 12

# Device Management RESTful Web Services

- [Device Management RESTful Web Services on page 153](#)

## Device Management RESTful Web Services

---

The following operations can be performed using the Security Director Device Management RESTful Web Services.

### GET

This request is used to collect all the device related information.

URI	/api/juniper/sd/device-management/devices
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.device-management.devices+xml;q="0.01";version="1" application/vnd.juniper.sd.device-management.devices+json;q="0.01";version="1"
Consumes	None
Produces	Collection of device information

### Sample Device Management Output

The getAllDevice filtering is supported for name, device IP, and platform. The sorting is supported for name, device IP, platform, and software-release.

#### Sample XML Output

```
<devices uri="/api/juniper/sd/device-management/devices" total="1">
  <device uri="/api/juniper/sd/device-management/devices/32768" href=
"/api/juniper/sd/device-management/devices/32768" >
    <assigned-services/>
    <domain-id>2</domain-id>
    <domain-name>Global</domain-name>
    <installed-services/>
    <pending-services/>
    <cluster-id>0</cluster-id>
    <name>SRX-119-7</name>
```

```

<platform>SRX240B</platform>
<cems-moid>net.juniper.jmp.jpa.LogicalDevice:131098</cems-moid>
<moid>
net.juniper.jnap.sm.om.jpa.SecurityDeviceEntity:32768
</moid>
<device-ip>10.205.119.7</device-ip>
<device-family>junos-es</device-family>
<software-release>12.1I20131010_srx_12q1_x46_intgr.0-608229</software-release>
<id>32768</id>
</device>
</devices>

```

### Sample Device Management Input and Output to Get Device by ID

URI: /api/juniper/sd/device-management/devices/328456

#### Sample XML Output

```

<device uri="/api/juniper/sd/device-management/devices/32768">
<domain-id>2</domain-id>
<domain-name>Global</domain-name>
<management-status>UNMANAGED</management-status>
<name>SRX-119-7</name>
<platform>SRX240B</platform>
<cems-moid>net.juniper.jmp.jpa.LogicalDevice:131098</cems-moid>
<moid>
net.juniper.jnap.sm.om.jpa.SecurityDeviceEntity:32768
</moid>
<assigned-services/>
<device-ip>10.205.119.7</device-ip>
<cluster-id>0</cluster-id>
<configuration-status>In Sync</configuration-status>
<connection-status>up</connection-status>
<device-family>junos-es</device-family>
<software-release>12.1I20131010_srx_12q1_x46_intgr.0-608229</software-release>
<virtual-chassis-status>>false</virtual-chassis-status>
<cc-status>Does Not Exist</cc-status>
<pending-services/>
<installed-services/>
<id>32768</id>
<Zone rel="Zones for this device" href=
"/api/juniper/sd/device-management/devices/32768/zones" />
<Interfaces rel="Interfaces for this device" href=
"/api/juniper/sd/device-management/devices/32768/interfaces" />
<routing-instances rel="Routing instances for this device" href=
"/api/juniper/sd/device-management/devices/32768/routing-instances" />
</device>

```

### Sample Device Management Input and Output to Get Zones of a Security Director Managed Devices

URI: /api/juniper/sd/device-management/devices/328456/zones

#### Sample XML Output

```

<zones total="5" uri="/api/juniper/sd/device-management/devices/426240/zones">
<zone>
<name>trust</name>
<interfaces total="0">
<interface>ge-0/0/0.0</interface>

```



```

<interface>ge-0/0/1.0</interface>
<interface>st0.10</interface>
<interface>st0.12</interface>
</interfaces>
</zone>
<zone>
<name>untrust</name>
<interfaces total="0">
<interface>ge-0/0/3.0</interface>
<interface>st0.2</interface>
<interface>ge-0/0/2.0</interface>
<interface>st0.4</interface>
<interface>st0.3</interface>
</interfaces>
</zone>
<zone>
<name>Untrust</name>
<interfaces total="0"/>
</zone>
<zone>
<name>zone-10161</name>
<interfaces total="0"/>
</zone>
<zone>
<name>junos-host</name>
<interfaces total="0"/>
</zone>
</zones>

```

### Sample Device Management Input and Output to Get Routing Instances of a Security Director Managed Devices

URI: /api/juniper/sd/device-management/devices/98939/interfaces

#### Sample XML Output

```

<interfaces total="4"
uri="/api/juniper/sd/device-management/devices/98939/interfaces">
  <interface>
    <cems-moid>net.juniper.jmp.jpa.LogicalDevice:294918</cems-moid>
    <edge-point>false</edge-point>
    <is-loopback>false</is-loopback>
    <managed-element>
      <id>0</id>
    </managed-element>
    <ip-addr>10.205.119.4</ip-addr>
    <ip-netmask>16</ip-netmask>
    <ptp>
      <edge-point>false</edge-point>
      <is-loopback>false</is-loopback>
      <speed>0</speed>
      <mtu>0</mtu>
      <id>0</id>
    </ptp>
    <is-management>false</is-management>
    <family>inet</family>
    <unit>0</unit>
    <id>327684</id>
  </interface>

```

```
<name>ge-0/0/0.0</name>
</interface>
<interface>
  <cems-moid>net.juniper.jmp.jp LogicalDevice:294918</cems-moid>
  <edge-point>>false</edge-point>
  <is-loopback>>false</is-loopback>
  <managed-element>
    <id>0</id>
  </managed-element>
  <ip-addr>198.51.100.2</ip-addr>
  <ip-netmask>16</ip-netmask>
  <ptp>
    <edge-point>>false</edge-point>
    <is-loopback>>false</is-loopback>
    <speed>0</speed>
    <mtu>0</mtu>
    <id>0</id>
  </ptp>
  <is-management>>false</is-management>
  <family>inet</family>
  <unit>0</unit>
  <id>327692</id>
  <name>ge-0/0/1.0</name>
</interface>
<interface>
  <cems-moid>net.juniper.jmp.jp LogicalDevice:294918</cems-moid>
  <edge-point>>false</edge-point>
  <is-loopback>>false</is-loopback>
  <managed-element>
    <id>0</id>
  </managed-element>
  <ip-addr>198.51.100.3</ip-addr>
  <ip-netmask>16</ip-netmask>
  <ptp>
    <edge-point>>false</edge-point>
    <is-loopback>>false</is-loopback>
    <speed>0</speed>
    <mtu>0</mtu>
    <id>0</id>
  </ptp>
  <is-management>>false</is-management>
  <family>inet</family>
  <unit>0</unit>
  <id>327694</id>
  <name>ge-0/0/2.0</name>
</interface>
<interface>
  <cems-moid>net.juniper.jmp.jp LogicalDevice:294918</cems-moid>
  <edge-point>>false</edge-point>
  <is-loopback>>false</is-loopback>
  <managed-element>
    <id>0</id>
  </managed-element>
  <ip-addr>198.51.100.3</ip-addr>
  <ip-netmask>16</ip-netmask>
  <ptp>
```

```

<edge-point>false</edge-point>
<is-loopback>false</is-loopback>
<speed>0</speed>
<mtu>0</mtu>
<id>0</id>
</ptp>
<is-management>false</is-management>
<family>inet</family>
<unit>0</unit>
<id>327696</id>
<name>ge-0/0/3.0</name>
</interface>
</interfaces>

```

### Sample Device Management Input and Output to Get routing instances of a Security Director Managed Devices

URI: /api/juniper/sd/device-management/devices/98939/routing-instances

#### Sample XML Output

```

<routing-instances total="2"
uri="/api/juniper/sd/device-management/devices/98939/routing-instances">
  <routing-instance>
    <instance-type>VIRTUAL_ROUTER</instance-type>
    <vpls>
      <vpls-id>0</vpls-id>
      <no-tunnel-services>false</no-tunnel-services>
      <id>0</id>
    </vpls>
    <device-name>294918</device-name>
    <id>327740</id>
    <name>vr1</name>
  </routing-instance>
  <routing-instance>
    <instance-type>VIRTUAL_ROUTER</instance-type>
    <vpls>
      <vpls-id>0</vpls-id>
      <no-tunnel-services>false</no-tunnel-services>
      <id>0</id>
    </vpls>
    <device-name>294918</device-name>
    <id>327741</id>
    <name>vr2</name>
  </routing-instance>
</routing-instances>

```

## POST

This request is used to schedule a job to update the particular device and return the job parameters.

URI	api/juniper/sd/device-management/update-devices
HTTP Method	HTTP POST

Content-Type	application/vnd.juniper.sd.device-management.update-devices+xml;version=1;charset=UTF-8 application/vnd.juniper.sd.device-management.update-devices+json;version=1;charset=UTF-8
Consumes	None
Produces	Schedules a job and returns the job paramters

To update the device, send the update information to the Junos Space server, as shown in the following example.

URI: api/juniper/sd/device-management/update-devices

#### Sample XML Input

```
<update-devices>
  <sd-ids>
    <id>99118</id>
  </sd-ids>
  <service-types>
    <service-type>POLICY</service-type>
  </service-types>
  <update-options>
    <enable-policy-rematch-srx-only>boolean</enable-policy-rematch-srx-only>
  </update-options>
</update-devices>
```

If you want to schedule the update after a particular time, send the information as shown in the following example.

URI: api/juniper/sd/device-management/update-devices?schedule=(after(00 01 30))

The syntax for scheduling after a particular time period is schedule=(after(dd HH mm)) or schedule=(after(HH mm)).

- dd—Days (optional parameter)
- HH—Hours
- mm—Minutes

The syntax for scheduling a job at a particular time is schedule= (at(ss mm HH dd MM ? yy)).

- ss—Seconds (mandatory field)
- mm—Minutes (mandatory field)
- HH—Hours (mandatory field)
- dd—Day of the month (mandatory field)
- EE—Day of week (mandatory field)
- MM—Month (mandatory field)
- yy—Year (optional field)
- ?—This is the allowed value of EE.

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)



## PART 5

# Security Director Job Management

- [Job Management RESTful Web Services on page 163](#)





## CHAPTER 13

# Job Management RESTful Web Services

- Job Management RESTful Web Services on page 163

## Job Management RESTful Web Services

---

The following operations can be performed using the Security Director Job Management RESTful Web Services.

### GET

This request is used to get all job information of a device in Security Director.

URI	api/juniper/sd/job-management/jobs/{job-id}/device-results
HTTP Method	HTTP GET
Content-Type	application/vnd.juniper.sd.job-management.device-results+xml;version=1;q=0.01 application/vnd.juniper.sd.job-management.device-results+json;version=1;q=0.01
Consumes	None
Produces	Returns the device specific status for a particular update job.

### Sample XML Output

```
<device-results total="1"
uri="/api/juniper/sd/job-management/jobs/131109/device-results/">
  <device-result>
    <associated-service-name-list total="0">
      <associated-service-name-list>testVPN</associated-service-name-list>
      <associated-service-name-list>dev123</associated-service-name-list>
    </associated-service-name-list>
    <device-ip>198.51.100.1</device-ip>
    <hub>>false</hub>
    <job-result-id>491524</job-result-id>
    <warning-messages total="0"/>
    <job-instance-id>131109</job-instance-id>
    <status>SUCCESS</status>
    <device-name>sd-srx210-119.25</device-name>
    <Configuration href=
"/api/juniper/sd/job-management/jobs/131109/device-results/491524" />
```

```

    </device-result>
  </device-results>

```

### Sample Input and Output Showing Configuration of the Update Job

URI: api/juniper/sd/job-management/jobs/{job-id}/device-results/{job-result-id}

#### Sample XML Output

```

<configurations total="1"
uri="/api/juniper/sd/job-management/jobs/131109/device-results/491524">
  <configuration>
    <edit-config>
      <?xml version="1.0" encoding="UTF-8"?>
      <configuration>
        <applications>
          <application operation="create">
            <name>apple-ichat-snatmap</name>
            <destination-port>5678</destination-port>
            <protocol>udp</protocol>
          </application>
          <application-set operation="create">
            <name>apple-ichat</name>
            <application>
              <name>junos-aol</name>
            </application>
            <application>
              <name>apple-ichat-snatmap</name>
            </application>
            <application>
              <name>junos-https</name>
            </application>
            <application>
              <name>junos-sip</name>
            </application>
            <application>
              <name>junos-http</name>
            </application>
          </application-set>
        </applications>
        <interfaces>
          <interface>
            <name>st0</name>
            <unit operation="create">
              <name>2</name>
              <family>
                <inet/>
              </family>
            </unit>
          </interface>
        </interfaces>
        <security>
          <ike>
            <gateway operation="create">
              <name>sd-srx100-24_testVPN</name>
              <dead-peer-detection>
                <interval>10</interval>
                <threshold>5</threshold>

```

```

</dead-peer-detection>
<external-interface>lo0.0</external-interface>
<ike-policy>sd-srx100-24_testVPN</ike-policy>
<nat-keepalive>5</nat-keepalive>
<address>10.205.119.24</address>
</gateway>
<policy operation="create">
  <name>sd-srx100-24_testVPN</name>
  <mode>main</mode>
  <pre-shared-key>
    <ascii-text>#####</ascii-text>
  </pre-shared-key>
  <proposal-set>standard</proposal-set>
</policy>
</ike>
<ipsec>
  <policy operation="create">
    <name>testVPN</name>
    <proposal-set>standard</proposal-set>
  </policy>
  <vpn operation="create">
    <name>sd-srx100-24_testVPN</name>
    <bind-interface>st0.2</bind-interface>
    <ike>
      <gateway>sd-srx100-24_testVPN</gateway>
      <idle-time>60</idle-time>
      <install-interval>1</install-interval>
      <ipsec-policy>testVPN</ipsec-policy>
      <no-anti-replay/>
    </ike>
  </vpn>
</ipsec>
<policies>
  <policy>
    <from-zone-name>trust</from-zone-name>
    <to-zone-name>untrust</to-zone-name>
    <policy operation="delete">
      <name>Device-Zone-1</name>
    </policy>
    <policy>
      <name>Device-Zone-2</name>
      <match>
        <source-address operation="delete">any</source-address>
        <source-address>ad2</source-address>
      </match>
      <then>
        <log>
          <session-init/>
        </log>
      </then>
    </policy>
    <policy operation="create">
      <name>aDevice-Zone-3</name>
      <match>
        <application>any</application>
        <destination-address>ad1</destination-address>

```

```
<source-address>any</source-address>
</match>
<then>
  <log>
    <session-close/>
  </log>
  <permit/>
</then>
</policy>
<policy name="Device-Zone-3" insert="before">
  <name>aDevice-Zone-3</name>
</policy>
<policy>
  <name>Device-Zone-3</name>
  <match>
    <application operation="delete">any</application>
    <application>apple-ichat</application>
    <source-address operation="delete">any</source-address>
    <source-address>ad2</source-address>
  </match>
  <then>
    <reject/>
  </then>
</policy>
</policies>
<zones>
  <security-zone>
    <name>trust</name>
    <address-book>
      <address operation="create">
        <name>ad2-mem0</name>
        <ip-prefix>192.0.2.0/24</ip-prefix>
      </address>
      <address operation="create">
        <name>ad2-mem1</name>
        <ip-prefix>192.0.2.1/24</ip-prefix>
      </address>
      <address operation="create">
        <name>ad2-mem2</name>
        <ip-prefix>192.0.2.2/24</ip-prefix>
      </address>
      <address operation="create">
        <name>ad2-mem3</name>
        <ip-prefix>192.0.2.3/24</ip-prefix>
      </address>
      <address operation="create">
        <name>ad2-mem4</name>
        <ip-prefix>192.0.2.4/24</ip-prefix>
      </address>
      <address operation="create">
        <name>ad2-mem5</name>
        <ip-prefix>192.0.2.5/24</ip-prefix>
      </address>
      <address operation="create">
        <name>ad2-mem6</name>
        <ip-prefix>192.0.2.5/24</ip-prefix>
      </address>
    </address-book>
  </security-zone>
</zones>
```

```

</address>
<address-set operation="create">
  <name>ad2</name>
  <address>
    <name>ad2-mem0</name>
  </address>
  <address>
    <name>ad2-mem1</name>
  </address>
  <address>
    <name>ad2-mem2</name>
  </address>
  <address>
    <name>ad2-mem3</name>
  </address>
  <address>
    <name>ad2-mem4</name>
  </address>
  <address>
    <name>ad2-mem5</name>
  </address>
  <address>
    <name>ad2-mem6</name>
  </address>
</address-set>
</address-book>
</security-zone>
<security-zone>
  <name>untrust</name>
  <address-book> <address operation="create">
    <name>ad1</name>
    <ip-prefix>192.0.2.6/24</ip-prefix>
  </address>
</address-book>
</security-zone>
<security-zone>
  <name>VPN</name>
  <interfaces operation="create">
    <name>st0.2</name>
  </interfaces>
</security-zone>
</zones>
</security>
</configuration>
</edit-config>

```

- Related Documentation**
- [Security Director RESTful Web Services Overview on page 3](#)
  - [Using Security Director RESTful Web Services on page 5](#)

