Junos® Space

Junos® Space RESTful API Reference for Security Director

Release

15.1R1

Modified: 2016-06-24

Copyright © 2016, Juniper Networks, Inc.
# Table of Contents

About the Documentation ........................................... xi
  Documentation and Release Notes ................................. xi
  Documentation Conventions ...................................... xi
  Documentation Feedback ........................................ xiii
  Requesting Technical Support ................................ xiv
  Self-Help Online Tools and Resources ............................. xiv
  Opening a Case with JTAC ....................................... xiv

## Part 1  Security Director RESTful Web Services Overview

### Chapter 1  Security Director RESTful Web Services Overview ............................ 3
  Security Director RESTful Web Services Overview ............ 3
  Using Security Director RESTful Web Services .................. 5
  Format and Conventions ........................................... 5
  Media Types ..................................................... 5

## Part 2  Security Director Objects

### Chapter 2  Address Management RESTful Web Services .......................... 9
  Address Management RESTful Web Services ..................... 9
  GET ......................................................... 9
  POST ............................................... 13
  PUT ............................................. 14
  DELETE ................................... 15
  PATCH ...................................... 15

### Chapter 3  Service Management RESTful Web Services .................. 17
  Service Management RESTful Web Services ..................... 17
  GET ......................................................... 17
  POST ............................................... 24
  PUT ............................................. 25
  DELETE ................................... 26
  PATCH ...................................... 26

### Chapter 4  Application Signature Management RESTful Web Services .......... 29
  Application Signature Management RESTful Web Services .... 29
  GET ......................................................... 29
  POST ............................................... 33
  PUT ............................................. 37
  DELETE ................................... 38
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>RESTful Web Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>IPS Management</td>
<td>GET</td>
</tr>
<tr>
<td>6</td>
<td>Variables Management</td>
<td>GET</td>
</tr>
<tr>
<td>7</td>
<td>Scheduler Management</td>
<td>GET</td>
</tr>
<tr>
<td>8</td>
<td>UTM Management</td>
<td>GET</td>
</tr>
</tbody>
</table>

**Chapter 5 IPS Management RESTful Web Services**

- **GET**: 41

**Chapter 6 Variables Management RESTful Web Services**

- **GET**: 43
- **POST**: 46
- **PUT**: 48
- **DELETE**: 49
- **PATCH**: 49

**Chapter 7 Scheduler Management RESTful Web Services**

- **GET**: 51
- **POST**: 53
- **DELETE**: 54
- **DELETE**: 55

**Chapter 8 UTM Management RESTful Web Services**

- **GET**: 57
- **POST**: 59
- **PUT**: 60
- **DELETE**: 61
- **Antispam Profile Management**
  - **GET**: 62
  - **POST**: 63
  - **PUT**: 63
  - **DELETE**: 64
- **Antivirus Profile Management**
  - **GET**: 64
  - **POST**: 66
  - **PUT**: 67
  - **DELETE**: 68
- **Content Filtering Profile Management**
  - **GET**: 68
  - **POST**: 70
  - **PUT**: 71
  - **DELETE**: 73
- **Web Filtering Profile Management**
  - **GET**: 73
  - **POST**: 75
  - **PUT**: 76
  - **DELETE**: 77
  - **PATCH**: 77
- **URL Pattern Management**
  - **GET**: 78
  - **POST**: 79
  - **PUT**: 80
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Profiles</td>
<td>144</td>
</tr>
<tr>
<td>GET</td>
<td>144</td>
</tr>
<tr>
<td>POST</td>
<td>145</td>
</tr>
<tr>
<td>PUT</td>
<td>148</td>
</tr>
<tr>
<td>PATCH</td>
<td>149</td>
</tr>
<tr>
<td>DELETE</td>
<td>150</td>
</tr>
<tr>
<td>Security Intelligence Management</td>
<td>153</td>
</tr>
<tr>
<td>Security Intelligence RESTful Web Services</td>
<td></td>
</tr>
<tr>
<td>Security Intelligence Controller Settings Management RESTful Web Services</td>
<td>153</td>
</tr>
<tr>
<td>GET</td>
<td>153</td>
</tr>
<tr>
<td>POST</td>
<td>155</td>
</tr>
<tr>
<td>PUT</td>
<td>156</td>
</tr>
<tr>
<td>Spotlight Secure Connector Management RESTful Web Services</td>
<td>157</td>
</tr>
<tr>
<td>Connector Configuration Management RESTful Web Services</td>
<td>157</td>
</tr>
<tr>
<td>POST</td>
<td>157</td>
</tr>
<tr>
<td>Connector Management RESTful Web Service</td>
<td>157</td>
</tr>
<tr>
<td>GET</td>
<td>157</td>
</tr>
<tr>
<td>Connector Trusted CA Management RESTful Web Services</td>
<td>159</td>
</tr>
<tr>
<td>GET</td>
<td>159</td>
</tr>
<tr>
<td>POST</td>
<td>160</td>
</tr>
<tr>
<td>DELETE</td>
<td>161</td>
</tr>
<tr>
<td>Connector Feed Update Status Management RESTful Web Services</td>
<td>161</td>
</tr>
<tr>
<td>Connector Feed Update Status Summary</td>
<td>163</td>
</tr>
<tr>
<td>Add or Modify Connector Device Association RESTful Web Service</td>
<td>163</td>
</tr>
<tr>
<td>POST</td>
<td>164</td>
</tr>
<tr>
<td>Device Feed Status Management RESTful Web Services</td>
<td>164</td>
</tr>
<tr>
<td>Update Device to Connector RESTful Web Services</td>
<td>165</td>
</tr>
<tr>
<td>Security Intelligence Information Source Management RESTful Web Services</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>165</td>
</tr>
<tr>
<td>POST</td>
<td>166</td>
</tr>
<tr>
<td>PUT</td>
<td>167</td>
</tr>
<tr>
<td>DELETE</td>
<td>168</td>
</tr>
<tr>
<td>Security Intelligence Policies Management RESTful Web Services</td>
<td>168</td>
</tr>
<tr>
<td>GET</td>
<td>169</td>
</tr>
<tr>
<td>POST</td>
<td>170</td>
</tr>
<tr>
<td>PUT</td>
<td>171</td>
</tr>
<tr>
<td>DELETE</td>
<td>172</td>
</tr>
<tr>
<td>Security Intelligence Profile Management RESTful Web Services</td>
<td>172</td>
</tr>
<tr>
<td>GET</td>
<td>172</td>
</tr>
<tr>
<td>POST</td>
<td>174</td>
</tr>
<tr>
<td>PUT</td>
<td>174</td>
</tr>
<tr>
<td>DELETE</td>
<td>175</td>
</tr>
<tr>
<td>Security Intelligence Dynamic Address Management RESTful Web Services</td>
<td>175</td>
</tr>
<tr>
<td>GET</td>
<td>175</td>
</tr>
<tr>
<td>POST</td>
<td>177</td>
</tr>
<tr>
<td>PUT</td>
<td>177</td>
</tr>
</tbody>
</table>
Part 5 Security Device Management
Chapter 13 Device Management RESTful Web Services............................... 181
  GET ................................................................................. 181
  POST ............................................................................ 185

Part 6 Security Director Job Management
Chapter 14 Job Management RESTful Web Services.............................. 191
  GET ................................................................................. 191
List of Tables

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Security Director RESTful Web Services Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Security Director RESTful Web Services Overview</td>
</tr>
<tr>
<td></td>
<td>Table 3: Media-Type String Format Parameters</td>
</tr>
</tbody>
</table>

- About the Documentation ........................................... xi
- Table 1: Notice Icons .................................................. xii
- Table 2: Text and Syntax Conventions ............................. xii
- Table 3: Media-Type String Format Parameters ................. 6
About the Documentation

- Documentation and Release Notes on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at 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 xii defines notice icons used in this guide.
### Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="i" /></td>
<td>Informational note Indicates important features or instructions.</td>
</tr>
<tr>
<td>![!] (exclamation mark)</td>
<td>Caution Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td><img src="lightning" alt="eclipse" /></td>
<td>Warning Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="laser" alt="laser" /></td>
<td>Laser warning Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td><img src="lightbulb" alt="tip" /></td>
<td>Tip Indicates helpful information.</td>
</tr>
<tr>
<td><img src="best_practice" alt="best practice" /></td>
<td>Best practice Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

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

### Table 2: Text and Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the <code>configure</code> command: <code>user@host&gt; configure</code></td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td><code>user@host&gt; show chassis alarms</code> No alarms currently active</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.</td>
<td>• A policy term is a named structure that defines match conditions and actions. • <em>Junos OS CLI User Guide</em> • RFC 1997, <em>BGP Communities Attribute</em></td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine’s domain name: <code>[edit] root@# set system domain-name domain-name</code></td>
</tr>
</tbody>
</table>
### Table 2: Text and Syntax Conventions (continued)

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

**GUI Conventions**

- **Bold text like this**
  - Represents graphical user interface (GUI) items you click or select.
  - In the Logical Interfaces box, select All Interfaces.
  - To cancel the configuration, click Cancel.

- **> (bold right angle bracket)**
  - Separates levels in a hierarchy of menu selections.
  - In the configuration editor hierarchy, select `Protocols>Osfp`.

---

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

Requesting Technical Support

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

- 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 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

```xml
<space>
  <services>
    <service rel="info" href="/api/info"/>
    <service rel="sd" href="/api/juniper/sd"/>
  </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+xml;version=1;q=0.01
            </representation>
            <representation>application/
              vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1;q=0.01
            </representation>
          </representations>
          </header>
        </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>
  </http-methods>
</XRD>
Using Security Director RESTful Web Services

Format and Conventions on page 5

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vendor&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>&lt;service&gt;</td>
<td>Name of the Junos Space-specific service. Service names are all lowercase alphanumeric tokens with hyphen separators.</td>
</tr>
<tr>
<td>&lt;type&gt;</td>
<td>Type of resource. Types are all lowercase alphanumeric tokens with hyphen separators.</td>
</tr>
<tr>
<td>&lt;syntax&gt;</td>
<td>Representation of the resource.</td>
</tr>
<tr>
<td>&lt;version&gt;</td>
<td>Version of the API; versions begin with the numeral 1.</td>
</tr>
</tbody>
</table>

**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

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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/address-management/addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
</tbody>
</table>
| 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

```xml
<addresses total="12" url="/api/juniper/sd/address-management/addresses">
  <address href="/api/juniper/sd/address-management/addresses/98932" url="/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"
```
Sample JSON Output

```json
{
    "addresses": [  
        {
            "@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

URL:/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"
  }
}
```

NOTE: By using the default GET address option, you can retrieve a maximum of 1000 addresses. If you need to retrieve addresses more than 1000 entries, you must use the pagination option.

Sample Address Management input and output with Pagination

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/address-management/addresses?paging=(limit eq 10)</td>
<td>The first 10 addresses in the first page are listed.</td>
</tr>
<tr>
<td>/api/juniper/sd/address-management/addresses?paging=(start eq 5, limit eq 10)</td>
<td>Starting from record 5, next 10 records are fetched.</td>
</tr>
</tbody>
</table>
Sample Address Management Input and Output with Filtering

**URI**: /api/juniper/sd/address-management/addresses?filter=(globaleq '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

```xml
<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>192.0.2.1</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>192.0.2.2</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>192.0.2.3</ip-address>
    <description>Third Address</description>
    <id>655618</id>
  </address>
</addresses>
```

**URI**: /api/juniper/sd/address-management/addresses?filter=(globaleq '192.0.2.1') to list addresses have IP address 192.0.2.1

### Sample XML Output

```xml
<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>192.0.2.1</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

```xml
<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>VPN_AD1</name>
    <address-type>IPADDRESS</address-type>
    <ip-address>192.0.2.1</ip-address>
    <description>First Address</description>
    <id>98932</id>
  </address>
</addresses>
```
<name>Any</name>
<address-type>ANY</address-type>
<description>Predefined any address</description>
</address>
</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.

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

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.
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.

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

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**

```xml
<address>
  <name>IXS_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

```xml
<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>
  <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.

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

PATCH

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

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

```xml
<diff>
  <replace sel="address/name">
    <name>AD1_patch</name>
  </replace>
  <replace sel="address/description">
    <description>description modified</description>
  </replace>
</diff>
```

**Sample XML Input to Patch Address Name**

```xml
<diff>
  <replace sel="address/name">
    <name>AD1_patch</name>
  </replace>
</diff>
```

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

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

**Sample XML Input**

```xml
<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.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/service-management/services</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.service-management.services+xml;version=1;q=0.01</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.service-management.services+json;version=1;q=0.01</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of services</td>
</tr>
</tbody>
</table>

Sample Service Management Output

Sample XML Output

```
<services total="223" url="/api/juniper/sd/service-management/services">
  <service href="/api/juniper/sd/service-management/services/98304" url="/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" url="/api/juniper/sd/service-management/services/98305" />
  <id>98305</id>
  <name>ftp</name>
```
<description>predefined service</description>
</is-group>
</service>
<service href="/api/juniper/sd/service-management/services/98307"
uri="/api/juniper/sd/service-management/services/98307" id="98307">
<name>tftp</name>
<description>predefined service</description>
</is-group>
</service>
<service href="/api/juniper/sd/service-management/services/98309"
uri="/api/juniper/sd/service-management/services/98309" id="98309">
<name>rtsp</name>
<description>predefined service</description>
</is-group>
</service>
<service href="/api/juniper/sd/service-management/services/98311"
uri="/api/juniper/sd/service-management/services/98311" id="98311">
<name>netbios-session</name>
<description>predefined service</description>
</is-group>
</service>
<service href="/api/juniper/sd/service-management/services/99014"
uri="/api/juniper/sd/service-management/services/99014" id="99014">
<name>sun-rpc-any</name>
<description>
</description>
</is-group>true</is-group>
</service>
</services>

Sample JSON Output
{
  "services": [
    {"@href": "/api/juniper/sd/service-management/services/99014",
    "@uri": "/api/juniper/sd/service-management/services/99014",
    "id": 99014,
    "name": "sun-rpc-any",
    "description": "Sun RPC Any",
    "is-group": true
  }
]
Sample Service Management Input and Output to get service by ID

URL:/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">
        <url>/api/juniper/sd/service-management/services/98307/members"/>
    </members>
</service>
```

Sample JSON Output

```
{
    "service": {
        "@uri": "/api/juniper/sd/service-management/services/6954",
        "createdTime": "2012-10-16T05:26:09Z",
        "description": "predefined application",
        "id": 6954,
        "is-group": false,
        "name": "ms-rpc-any",
        "description": "",
        "is-group": true
    }
}
```
Sample Service Management Input and Output with Pagination

URI: /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">
    <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">
    <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">
    <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">
    <name>bootps</name>
    <description>predefined service</description>
    <is-group>false</is-group>
  </service>
  ...
</services>
```
Sample JSON Output

```json
{
  "services": [
    {
      "@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
    }
  ]
}
```
Sample Service Management Input and Output with Filtering

URI:/api/juniper/sd/service-management/services?filter=(globaleq '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

```xml
<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

```json
{
  "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

```xml
<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>
</service>
</service>
</service>
</service>

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

Services are listed in a descending order.

Sample XML Output

<services total="223" url="/api/juniper/sd/service-management/services">
  <service href="/api/juniper/sd/service-management/services/98558" url="/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/98560" url="/api/juniper/sd/service-management/services/98560">
    <id>98560</id>
    <name>wxcontrol</name>
    <description>predefined service</description>
  </service>
</services>
<is-group>false</is-group>
</service>

<service href="/api/juniper/sd/service-management/services/98554" url="/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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/service-management/services</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td><a href="application/vnd.juniper.sd.service-management.service+xml;version=1;charset=UTF-8">application/vnd.juniper.sd.service-management.service+xml;version=1;charset=UTF-8</a></td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Creates a new service</td>
</tr>
</tbody>
</table>

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.

```xml
<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>
</service>
```
**PUT**

This request is used to modify a service.

**URI**
/api/juniper/sd/service-management/services/{service-id}

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>HTTP PUT</th>
</tr>
</thead>
</table>

| 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.

```xml
<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>
  </protocol>
</service>
```
2. Required fields are modified in a service.

DELETE

This request is used to delete a service.

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

PATCH

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

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

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

Sample XML Input 2

```xml
<!--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

```xml
<!--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

```xml
<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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/app-sig-management</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.app-sig-management+xml;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.app-sig-management+json;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of application signatures</td>
</tr>
</tbody>
</table>

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

URL: /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

```xml
<app-sigs total="1751" url="/api/juniper/sd/app-sig-management/app-sigs">
  <display-name>MISC: Finger Protocol</display-name>
  <definition-type>PREDEFINED</definition-type>
  <id>361</id>
  <name>FINGER</name>
</app-sigs>
```
Sample Application Signature Management Input and Output to Get Application Signature by ID

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

Sample XML Output

```xml
<app-sig url="/api/juniper/sd/app-sig-management/app-sigs/361" edit-version="0" definition-type="PREDEFINED" id="361">
  <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>
    </pattern-set>
  </pattern-sets>
</app-sig>
```
<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>
</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" url="/api/juniper/sd/app-sig-management/app-sigs">
  <app-sig href="/api/juniper/sd/app-sig-management/app-sigs/361" url="/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" url="/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>
    <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" url="/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**

<table>
<thead>
<tr>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/app-sig-management/app-sigs?paging=(limit eq 10)</td>
<td>Ten application signatures are listed</td>
</tr>
<tr>
<td>/api/juniper/sd/app-sig-management/app-sigs?paging=(start eq 100, limit eq 10)</td>
<td>From record number 100, ten application signatures are listed.</td>
</tr>
</tbody>
</table>
POST

This request is to create a new application signature.

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

Creating a New Application Signature in Basic Mode

Sample XML Input

```xml
<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>Character</value>
    </idp-common-value>
  </app-sig-tags>
</app-sig>
```
Creating a New Application Signature in Advanced Mode

Sample XML Input

```xml
<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>
        </pattern-member>
      </members>
    </pattern-set>
  </pattern-sets>
</app-sig>
```
<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>cts</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/>

Copyright © 2016, Juniper Networks, Inc.
Creating a Custom Application Signature Group

Sample XML Input

```xml
<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>
```
PUT

This request is to modify the application signature.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/app-sig-management/app-sigs</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PUT</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.app-sig-management.app-sig+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Modifies the application signature.</td>
</tr>
</tbody>
</table>

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

Sample XML Input

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

This request is to delete the application signature.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/app-sig-management/app-sigs/&lt;app-sig id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.app-sig-management.app-sig+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.app-sig-management.app-sig+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes the application signature.</td>
</tr>
</tbody>
</table>
Related Documentation

- Security Director RESTful Web Services Overview on page 3
- Using Security Director RESTful Web Services on page 5
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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/ips-management/ips-sig-sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.ips-management.ips-sig-sets+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of IPS signature sets</td>
</tr>
</tbody>
</table>

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

Sample XML Output

```xml
<ips-sig-sets total="9" uri="/api/juniper/sd/ips-management/ips-sig-sets">
    <name>Web_Server (Predefined) (29)</name>
    <definition-type>PREDEFINED</definition-type>
    <description>This template policy is designed to protect commonly used HTTP servers from remote attacks.</description>
  </ips-sig-set>
</ips-sig-sets>
```
DMZ_Services (Predefined) (40)
<description>This template policy is designed to be used to protect a typical DMZ environment.</description>
<definition-type>PREDEFINED</definition-type>
</ips-sig-set>

DNS_Service (Predefined) (11)
<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>
</ips-sig-set>

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

Web_Server (Predefined)
<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>
<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 collected all the variables configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/variable-management/variable-definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
</tbody>
</table>
| 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

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

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

Sample XML output to get polymorphic address by ID

Copyright © 2016, Juniper Networks, Inc.
Sample XML output to get polymorphic zone by ID

```
<variable-definition
  url="/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>
    <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>
  </default-value-detail>
</variable-definition>
```

Sample Variable Management Input and Output with Pagination

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

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" url="/api/juniper/sd/variable-management/variable-definitions">
  <variable-definition
  url="/api/juniper/sd/variable-management/variable-definitions/33470">
```
Sample Variable Management Input and Output with Sorting

<table>
<thead>
<tr>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/variable-management/variable-definitions?sortby=(name(ascending))</td>
<td>All variable definition names are sorted in an ascending order.</td>
</tr>
<tr>
<td>/api/juniper/sd/variable-management/variable-definitions?sortby=(name(ascending))</td>
<td>All variable definition names are sorted in an descending order.</td>
</tr>
</tbody>
</table>

POST

This request is used to create a variable.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/variable-management/variable-definitions</th>
</tr>
</thead>
</table>

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

None Consumes

Creates a new variable definition

Sample XML Input

```xml
  <variable-definition>
    <variable-values-list>
      <variable-values>
        <device>
          <moid>net.juniper.jmp.jpa.LogicalDevice:327752</moid>
          <name>sd-srx240-2</name>
        </device>
      </variable-values>
    </variable-values-list>
  </variable-definition>
```
The following example shows creation of polymorphic zone:

Sample XML Input

```xml
<variable-definition>
    <name>var_zone1</name>
    <created-by-user-name>super</created-by-user-name>
    <definition-type>CUSTOM</definition-type>
    <type>ZONE</type>
    <description>variable zone created using REST</description>
    <default-name>trust</default-name>
    <variable-values-list>
        <variable-values>
            <id/>
            <device>
                <moid>net.juniper.jmp.jpa.LogicalDevice:327748</moid>
                <name>sd-srx650-4</name>
            </device>
        </variable-values>
        <variable-value-detail>
            <variable-value>trust</variable-value>
            <name>trust</name>
        </variable-value-detail>
    </variable-values-list>
</variable-definition>
```
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**
```xml
<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 href="/api/juniper/sd/address-management/addresses/1016194">
          <default-value>net.juniper.jnap.sm.om.jpa.AddressEntity:1016194</default-value>
          <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>
        </variable-value-detail>
      </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>
    <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>
  </default-value-detail>
  <name>var_add1</name>
  <edit-version>0</edit-version>
</variable-definition>
```
<description>variable address created using REST</description>
<default-name>User_AD1</default-name>
</variable-definition>

## DELETE

This request is used to delete a variable.

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

## PATCH

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

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

### 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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/scheduler-management/schedulers/</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.scheduler-management.scheduler+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.scheduler-management.scheduler+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Lists schedulers</td>
</tr>
</tbody>
</table>

Sample XML Output

```xml
<schedulers total="4" url="/api/juniper/sd/scheduler-management/schedulers/">
  <scheduler href="/api/juniper/sd/scheduler-management/schedulers/426244" url="/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" url="/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" url="/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 Pagination:

<table>
<thead>
<tr>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/scheduler-management/schedulers?paging=(limit eq 3)</td>
<td>The first 3 schedulers in the first page are listed.</td>
</tr>
<tr>
<td>/api/juniper/sd/scheduler-management/schedulers?paging=(start eq 1, limit eq 2)</td>
<td>Start with record number 1 next 2 records are fetched</td>
</tr>
</tbody>
</table>

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

```xml
<schedulers total="4" url="/api/juniper/sd/scheduler-management/schedulers/">
    <scheduler href="/api/juniper/sd/scheduler-management/schedulers/426244" url="/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" url="/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" url="/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" url="/api/juniper/sd/scheduler-management/schedulers/426250">
        <name>scheduler_3</name>
        <description>scheduler_2</description>
        <id>426250</id>
    </scheduler>
</.schedulers>
```
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

<table>
<thead>
<tr>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/scheduler-management/schedulers?sortBy=(name(ascending))</td>
<td>Scheduler names are listed in an ascending order.</td>
</tr>
<tr>
<td>/api/juniper/sd/scheduler-management/schedulers?sortBy=(name(descending))</td>
<td>Scheduler names are listed in descending order.</td>
</tr>
</tbody>
</table>

POST

This request is used to create a new scheduler.

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

Sample XML Input

<scheduler>
  <name>scheduler_1</name>
  <description>scheduler_1</description>
  <start-date>2013-04-10.23:23</start-date>
  <stop-date>2013-04-12.12:12</stop-date>
  <start-date>2013-04-16.03:23</start-date>
  <stop-date>2013-04-18.04:12</stop-date>
  <schedules>
    <schedule>
      <day>MONDAY</day>
      <start-time1/>
      <stop-time1/>
      <start-time2/>
      <stop-time2/>
      <exclude>true</exclude>
    </schedule>
  </schedules>
</scheduler>
Modify a Scheduler

This request is used to modify an existing scheduler.

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

**Sample XML Input**

```xml
<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">

```

```xml
<schedule>
<day>TUESDAY</day>
<start-time1 />
<stop-time1 />
<start-time2 />
<stop-time2 />
<exclude>true</exclude>
<all-day>true</all-day>
</schedule>
</schedules>
</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 |
| None | 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.

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

Sample XML Output

```xml
<utm-policies url="/api/juniper/sd/utm-management/utm-policies" total="9">
  <utm-policy href="/api/juniper/sd/utm-management/utm-policies/98542" url="/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>
  </utm-policy>
</utm-policies>
```
Sample Input and Output to Get UTM Policies by ID

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

Sample XML Output:

```xml
<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.

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

**Sample XML Input**

```xml
<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>
  </anti-virus-profiles>
</utm-policy>
```
PUT

This request is used to modify UTM policy.

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

**Sample XML Input**

```xml
<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>
```
DELETE

This request is used to delete UTM policy.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/utm-policies/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.utm-policy+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.utm-policy+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
</tbody>
</table>
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">
    <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>

    <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>
  </anti-spam-profile>
</anti-spam-profiles>
```
### POST

This request is used to create a new antispam profile.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>api/juniper/sd/utm-management/anti-spam-profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP POST</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.utm-management.anti-spam-profile+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.anti-spam-profile+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td><strong>Consumes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Produces</strong></td>
<td>Create a new antispam profile.</td>
</tr>
</tbody>
</table>

**Sample XML Input**

```xml
<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 antispam profile.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>api/juniper/sd/utm-management/anti-spam-profiles/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP PUT</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.utm-management.anti-spam-profile+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.anti-spam-profile+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td><strong>Consumes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Produces</strong></td>
<td>Modifies an antispam profile.</td>
</tr>
</tbody>
</table>

**Sample XML Input**

```xml
<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.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/anti-spam-profiles/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.anti-spam-profile+xml;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.anti-spam-profile+json;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes an antispam profile.</td>
</tr>
</tbody>
</table>

**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.

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

**Sample XML Output**

```xml
<anti-virus-profiles uri="/api/juniper/sd/utm-management/anti-virus-profiles" total="6">
    <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-profiles>
```
   <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>
</anti-virus-profile>
POST

This request is used to create a new antivirus profile.

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

sample XML Input

```xml
<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>
    <fallback-non-block-notification-option>
      <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-option>
    <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-options>
  </fallback-non-block-notification-options>
</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**

```xml
<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-options>
  <fallback-non-block-notification-options>
    <custom-notification-message>This is blocked</custom-notification-message>
    <custom-notification-subject>This is blocked</custom-notification-subject>
  </fallback-non-block-notification-options>
</anti-virus-profile>
```
<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>
</fallback-options>
<profile-type>KASPERSKY</profile-type>
</anti-virus-profile>

DELETE

This request is used to delete an antivirus profile.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/anti-virus-profiles/[id]</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.anti-virus-profile+xml;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.anti-virus-profile+json;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes an antivirus profile.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/utm-management/content-filtering-profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| 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+jason;version=1;q=0.01 |
| Consumes | None |
| Produces | Collection of content filtering objects. |

**Sample XML Output**

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

**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
url="/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-list>
```
POST

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

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

---

 Junos Space RESTful API Reference for Security Director

Copyright © 2016, Juniper Networks, Inc.
Sample XML Input

```xml
<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]
<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>HTTP PUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.content-filtering-profile+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.content-filtering-profile+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Modifies the content filtering profile.</td>
</tr>
</tbody>
</table>

**Sample XML Input**

```xml
<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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/utm-management/content-filtering-profiles/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.content-filtering-profile+xml;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.content-filtering-profile+json;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes the content filtering profile.</td>
</tr>
</tbody>
</table>

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.

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

Sample XML Output

```xml
<web-filtering-profiles uri="/api/juniper/sd/utm-management/web-filtering-profiles" total="10">
    <name>wf-cpa-default</name>
    <domain-name>SYSTEM</domain-name>
    <domain-id>1</domain-id>
  </web-filtering-profile>
</web-filtering-profiles>
```
Sample Input and Output to Get Web Profiles by ID

URL: api/juniper/sd/utm-management/web-filtering-profiles

Sample XML Output

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

**POST**

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

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

**Sample XML Input**

```xml
<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-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>
  </site-reputation-actions>
</web-filtering-profile>
```
PUT

This request is used to modify web filtering profile.

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>HTTP PUT</th>
</tr>
</thead>
</table>
| 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**

```xml
<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>
      <url-category-list>
        <id>98427</id>
        <name>Enhanced_Internet_Telephony</name>
      </url-category-list>
    </url-category-action>
  </url-category-action-list>
</web-filtering-profile>
```
<reputation-action/>
<url-category-list>
  <id>98422</id>
  <name>Enhanced_Pay_to_Surf</name>
</url-category-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.

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

PATCH

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

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/web-filtering-profiles/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PATCH</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.web-filtering-profile_patch+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.web-filtering-profile_patch+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Creates or modifies a web filtering profile.</td>
</tr>
</tbody>
</table>
Sample XML Input for Adding a New Category

```xml
<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

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

Sample XML Input for Replacing With New Sets of Category

```xml
<diff>
  <replace sel="web-filtering-profile/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>
  </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.

<table>
<thead>
<tr>
<th>URI</th>
<th>HTTP Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/utm-management/url-patterns</td>
<td>HTTP GET</td>
</tr>
</tbody>
</table>
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>
        <name>Pattern-Block-List</name>
      </url-pattern>
    </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.

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

Sample XML Input

<url-pattern>
  <name>Pattern-Block-List</name>
</url-pattern>
<description>This object is created using REST</description>

```xml
<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>
```

**PUT**

This request is used to modify the URL pattern.

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

**Sample XML Input**

```xml
<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.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/url-patterns/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.url-patterns+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.url-patterns+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes the URL pattern.</td>
</tr>
</tbody>
</table>
**PATCH**

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

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

**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.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/url-category-lists</th>
</tr>
</thead>
</table>

---

Copyright © 2016, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>HTTP GET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.utm-management.url-category-list-refs+xml;version=1</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.url-category-list-refs+json;version=1</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of URL category objects.</td>
</tr>
</tbody>
</table>

**Sample XML Output**

```xml
<url-category-lists uri="/api/juniper/sd/utm-management/url-category-lists" total="175">
    <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>
</url-category-lists>
```

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

**URI:** api/juniper/sd/utm-management/url-category-lists/[id]

**Sample XML Output**

```xml
<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.jpa.EmailAddressPatternEntity:99562
      </moid>
    </url-pattern>
  </url-patterns>
</url-category-list>
```
POST

This request is used to create a URL category list.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>api/juniper/sd/utm-management/url-category-lists</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP POST</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.utm-management.url-category-list+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.url-category-list+json;version=1;charset=UTF-8</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>api/juniper/sd/utm-management/url-category-lists/[id]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP PUT</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.utm-management.url-category-list+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.utm-management.url-category-list+json;version=1;charset=UTF-8</td>
</tr>
</tbody>
</table>

**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>
```
DELETE

This request is used to delete the URL categories.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/url-category-lists/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/utm-management/url-category-lists/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PATCH</td>
</tr>
</tbody>
</table>
| 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

```xml
<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

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

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

**Sample XML Output**

```xml
<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"  
        url="/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**

```xml
<utm-device-profile href="/api/juniper/sd/utm-management/utm-device-profiles/99580"
url="/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 url="/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.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>api/juniper/sd/utm-management/utm-device-profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| 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**

```xml
<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.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>
</utm-device-profile>
```
**PUT**

This request is used to modify the device profile.

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

**sample XML Input**

```xml
<utm-device-profile>
  <name>Global-Setting</name>
  <description>This is created using REST</description>
  <edit-version>1</edit-version>
  <id>128830</id>
  <devices
  url="/api/juniper/sd/utm-management/utm-device-profiles/121520/devices">
    <device>
      <name>scale-6133</name>
      <moid>net.juniper.inap.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>
</utm-device-profile>
```
DELETE

This request is used to delete the device profile.

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

**Related Documentation**

- Security Director RESTful Web Services Overview on page 3
- Using Security Director RESTful Web Services on page 5
### 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.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/zoneset-management/zone-sets/&lt;zone-set id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP POST</td>
</tr>
</tbody>
</table>
| **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 |
| **Produce** | Creates a new zone set. |

**Sample Zone Set Creation Request Body**

```xml
<zone-set>
  <edit-version>1</edit-version>
  <zone-type>ZONESET</zone-type>
  <zones>
    internal_1,internal_2,internal_3,internal_4,internal_5
  </zones>
  <id></id>
  <description>created for testing multizone automation</description>
  <domain-id>3</domain-id>
  <name>Internal1111</name>
</zone-set>
```
## PUT

This request is to modify the zone set.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/zoneset-management/zone-sets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP PUT</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.zoneset-management.zone-set+json;version=1</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.zoneset-management.zone-set+xml;version=1</td>
</tr>
<tr>
<td><strong>Consumes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Produces</strong></td>
<td>Modifies a zone set.</td>
</tr>
</tbody>
</table>

### Sample XML Input

```xml
<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.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/zoneset-management/zone-sets/&lt;zone-set id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.zoneset-management.zone-set+json;version=1</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.zoneset-management.zone-set+xml;version=1</td>
</tr>
<tr>
<td><strong>Consumes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Produces</strong></td>
<td>Deletes the zone set</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/fwpolicy-management/firewall-policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.fwpolicy-management.firewall-policies+xml;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.fwpolicy-management.firewall-policies+JSON;version=1;q=0.01</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of firewall polices</td>
</tr>
</tbody>
</table>

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"
```

Copyright © 2016, Juniper Networks, Inc.
Sample JSON Output

```json
{
    "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

```xml
<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>
```
Sample Firewall Policy Management Input and Output to Get Policy by ID

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

Sample XML Output

```xml
<firewall-policy>
<name>AllDevicesPolicy</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

```json
{
    "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": [
   {"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.

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

Sample XML Output

<devices total="2"
   url="/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 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>
</firewall-rule>
```
<action>TUNNEL</action>
<vpn-tunnel-refs>
  <id>32775</id>
  <name>sd-srx110-119_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>
    </custom-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-srx110-119_25_pv</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=(globaleq '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

```xml
<firewall-policies total="1">
  <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

```json
{
  "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 a 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

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

```
<firewall-rule url="/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>
```
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"
url="/api/juniper/sd/fwpolicy-management/firewall-rules/32774/members">
<firewall-rule href="/api/juniper/sd/fwpolicy-management/firewall-rules/2195456"
url="/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"
url="/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"
url="/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

```xml
<custom-columns total="3">
  <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.

**URL:** /api/juniper/sd/fwpolicy-management/custom-columns

Sample XML Output

```xml
<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>
  </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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/fwpolicy-management/firewall-policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.fwpolicy-management.firewall-policy+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1;charset=UTF-8</td>
</tr>
</tbody>
</table>
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**

```xml
<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>
  <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**

```xml
<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>
</firewall-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>

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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/fwpolicy-management/firewall-policies/{policy-id}/lock</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.lock-management.lock+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.lock-management.lock+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Locks the firewall policy</td>
</tr>
</tbody>
</table>

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.

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

To publish a policy:

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

   **Sample XML Input**
   ```xml
   <publish>
   <policy-ids>
   <policy-id>
   1376291
   </policy-id>
   </policy-ids>
   </publish>
   ``

2. To publish and update the policy, use the URI:

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


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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/fwpolicy-management/firewall-policies/{policy-id}/assign-devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>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</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Assigns devices to the firewall policy</td>
</tr>
</tbody>
</table>

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

**Sample XML Input**

```xml
<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**

```xml
<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.

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

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

Sample XML Input
```xml
<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-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-addresses>
    </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

```xml
<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

```xml
<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-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-Any</id>
            <name>Any</name>
            <address-type>ANY</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/>
      </added-rule>
    </added-rules>
  </modify-rules>
</firewall-policy>
```
Chapter 10: Firewall Policy Management RESTful Web Services

/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>
</ips-enabled>
</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-SecIntell-Zone-Device Rules</rule-group-id>
/rule-type>RULE</rule-type>
/rule-order>0</rule-order>
/policy-name>FW-POLICY-SecIntell</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-SecIntell</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>
/zones-type>ZONE</zones-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>
/zones-type>ZONE</zones-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>
    <application-signature-type>NONE</application-signature-type>
    <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-SecIntell-Zone-Device Rules</rule-group-id>
    <rule-type>RULE</rule-type>
    <rule-order>0</rule-order>
    <policy-name>FW-POLICY-SecIntell</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-SecIntell</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>
    </added-rule>
  </added-rules>
</modify-rules>
<source-zones/>
<source-addresses/>
<source-address>
</id>0000addresses?include-dynamic-addresses=true-Dynamic-add1</id>
</name>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_ADDRESS_GROUP</address-type>
</destination-address>
<destination-analytics>
<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-SecIntell-Zone-Device Rules</rule-group-id>
<rule-type>RULE</rule-type>
<rule-order>0</rule-order>
<policy-name>FW-POLICY-SecIntell</policy-name>
<enabled>true</enabled>
<members/>
</added-rule>
<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>
<ips-mode>ADVANCED</ips-mode>
<ips-enabled>false</ips-enabled>
<scheduler />
<utm-policy />
<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>
</ips-enabled>
<scheduler />
<name>trust</name>
<zone-type>ZONE</zone-type>

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

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

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

```xml
<firewall-policy
  url="/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>
</firewall-policy>
```
<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>
<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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/fwpolicy-management/{policy-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.fwpolicy-management.firewall-policy+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.fwpolicy-management.firewall-policy+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes a policy</td>
</tr>
</tbody>
</table>
Policy Profiles

**GET**

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

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/fwpolicy-management/policy-profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP GET</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Consumes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Produces</strong></td>
<td>Collection of policy profiles</td>
</tr>
</tbody>
</table>

**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**

```xml
<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

<table>
<thead>
<tr>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/fwpolicy-management/policy-profiles?paging=(limit eq 10)</td>
<td>Ten policy profiles are listed.</td>
</tr>
<tr>
<td>/api/juniper/sd/fwpolicy-management/policy-profiles?paging=(start eq 10 limit eq 5)</td>
<td>From the record number 10, five policy profiles are listed.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/api/juniper/sd/fwpolicy-management/policy-profiles?sortby=(name(ascending))</td>
<td>All policy profile names are sorted in an ascending order.</td>
</tr>
<tr>
<td>/api/juniper/sd/fwpolicy-management/policy-profiles?sortby=(name(descending))</td>
<td>All policy profile names are sorted in an ascending order.</td>
</tr>
</tbody>
</table>

**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>
</policy-profile>
```
PUT

This request is used to modify a policy profile.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/fwpolicy-management/policy-profiles/{profile-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PUT</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.fwpolicy-management.policy-profile+xml;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.fwpolicy-management.policy-profile+JSON;version=1;q=0.01</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Modifies a policy profile</td>
</tr>
</tbody>
</table>

**Sample XML Modified Value**

```xml
<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>
  <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" |
| 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 |
| 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
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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/vpn-management</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.vpn-management.ipsec-vpns+xml;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.vpn-management.ipsec-vpns+json;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Links to manage IPsec VPN, Extranet, VPN Profile and Publish VPN</td>
</tr>
</tbody>
</table>

Sample VPN Management output

Sample XML Output

```xml
<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

```xml
<ipsec-vpns total="1" url="/api/juniper/sd/vpn-management/ipsec-vpns">
    <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>
  </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 this particular VPN to safe guard from the concurrent modification related issues.

Sample XML Output

```xml
<ipsec-vpns 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>
</ipsec-vpns>
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

```xml
<device>
  <certificate/>
</device>
<device>
  <certificate/>
</device>
```

Chapter 11: VPN Management RESTful Web Services

Copyright © 2016, Juniper Networks, Inc.

131
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 supports global search for searching on device name or device IP.

Sample XML Output

```xml
<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>
<device-moid>net.juniper.jnap.sm.om.jpa.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 XML Output

```

```xml
<devices>
  <device name="sd-srx240-2">
    <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>
      <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>192.0.2.0</local-proxyid>
      <remote-proxyid>192.0.2.1</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>
    </peer-device>
  </device>
</devices>
```
Sample VPN Management Input and Output with Pagination

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

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

```xml
<ipsec-vpns total="2" url="/api/juniper/sd/vpn-management/ipsec-vpns">
  <ipsec-vpn href="/api/juniper/sd/vpn-management/ipsec-vpns/32802" url="/api/juniper/sd/vpn-management/ipsec-vpns/32802/" id="32802">
    <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>
  </ipsec-vpn>
</ipsec-vpns>```
<vpn-tunnel-mode-types>ROUTE_BASED</vpn-tunnel-mode-types>  
<profile href="/api/juniper/sd/vpn-management/vpn-profiles/32815" />  
<name>CustomMainPre</name>  
</profile>  
<description>  
</description>  
</ipsec-vpn>  
</ipsec-vpns>  

URI: /api/juniper/sd/vpn-management/ipsec-vpns?filter=(globaleq'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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/vpn-management/devices?tunnelMode=&lt;tunnelMode&gt;&amp;isAutoVpn=true&amp;isAdvpn=false&amp;isMultiProxyID=false</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
</tbody>
</table>
| Content-Type | application/vnd.juniper.sd.vpn-management.devices+xml;version=2;q=0.02  
application/vnd.juniper.sd.vpn-management.devices+json;version=2;q=0.02 |
| 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>  
</vpn-mo>  
</create-vpn>
```
<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>1.1.0.0/24</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>
</vpn-device-bean>
<vpn-device-bean>
<is-hub>false</is-hub>
<external-if-name>reth0.0</external-if-name>
<proxy-id>1.3.0.0/24</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>
</vpn-device-bean>
</devices>

<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, VPN Profile ID, 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.

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

Sample XML Input

```xml
<modify-vpn>
  <vn-mo>
    <edit-version>1</edit-version>
    <id>491545</id>
    <name>vpn1</name>
    <description>Created by VPN Import workflow - BY API</description>
    <profile>
      <name>ImportVPNProfile_1</name>
      <id>491542</id>
    </profile>
    <advpn-settings/>
    <vn-tunnel-mode-types>ROUTE_BASED</vn-tunnel-mode-types>
    <type>SITE_TO_SITE</type>
    <tunnel-interface-type>NUMBERED</tunnel-interface-type>
    <tunnel-ip-range>
      <mask>24</mask>
      <network-ip>10.3.1.0</network-ip>
    </tunnel-ip-range>
    <tunnel-multi-point-size>-1</tunnel-multi-point-size>
    <max-transmission-unit>-1</max-transmission-unit>
    <publish-state>NOT_PUBLISHED</publish-state>
    <routing-type>STATIC</routing-type>
    <preshared-key-type>AUTO_GENERATE</preshared-key-type>
    <unique-key-per-tunnel>false</unique-key-per-tunnel>
    <preshared-key>$ABC123</preshared-key>
    <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>
    <advpn>false</advpn>
    <multi-proxyid>false</multi-proxyid>
  </vn-mo>
  <device-modification>
    <devices-to-modify>
      <vn-device-bean>
        <is-hub>false</is-hub>
        <ike-address>192.0.2.1</ike-address>
        <export-default-routes>false</export-default-routes>
        <export-static-routes>false</export-static-routes>
        <export-ospf-routes>false</export-ospf-routes>
      </vn-device-bean>
    </devices-to-modify>
  </device-modification>
</modify-vpn>
```
The following mandatory fields are required to modify a VPN:

- IPsec VPN ID
- VPN Profile 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

```xml
<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/>
    </vpn-end-point>
    <peer-device>
      <device-name>sd-srx650-4</device-name>
      <device-ip>10.207.97.137</device-ip>
    </peer-device>
  </end-points>

  <local-proxyid>192.0.2.5</local-proxyid>
  <remote-proxyid>192.0.2.6</remote-proxyid>
  <ike-id>198.51.100.2</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>
</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.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/vpn-management/publish</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
</tbody>
</table>
Send the publish information to the Junos Space server, as shown in the following example.

**Sample XML Input**

```xml
<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 DELETE

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>HTTP DELETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.vpn-management.delete+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes a VPN</td>
</tr>
</tbody>
</table>

### Extranet Devices

**GET**

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

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/vpn-management/extranet-devices</th>
</tr>
</thead>
</table>

**HTTP Method**

<table>
<thead>
<tr>
<th>HTTP GET</th>
</tr>
</thead>
</table>

| 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

```xml
<extranet-devices total="3" uri="/api/juniper/sd/vpn-management/extranet-devices">
    <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>
    <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>
    <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-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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/vpn-management/extranet-devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.vpn-management.extranet-device+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.vpn-management.extranet-device+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Creates a new extranet device</td>
</tr>
</tbody>
</table>

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>192.0.2.20</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 REST2</description>
</extranet-device>
```
PUT
This request is used to modify an extranet device.

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

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

**Sample XML Input**

```xml
<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>192.0.2.20</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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/vpn-management/extranet-devices/{extranet-device-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PATCH</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.vpn-management.extranet-device_patch+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.vpn-management.extranet-device_patch+json;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
</tbody>
</table>
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**

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

**Sample XML Input for Host**

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

**Sample XML Input for IP Address**

```xml
<diff>
  <replace sel=extranet-device/ip-address>
    <ip-address>192.0.2.20</ip-address>
  </replace>
  <replace sel=extranet-device/description>
    <description>description patched again</description>
  </replace>
</diff>
```

**Sample XML Input for Empty IP Address**

```xml
<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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/vpn-management/extranet-devices/[extranet-device-id]</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.vpn-management.extranet-devices+xml;q=0.01;version=1</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes an extranet device</td>
</tr>
</tbody>
</table>
## VPN Profiles

### GET

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

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

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

**Sample XML Output**

```xml
<vpn-profiles total="2" url="/api/juniper/sd/vpn-management/vpn-profiles">
    <name>MainModeProfile</name>
    <description>Predefined Main mode profile with Standard proposal set</description>
    <definition-type>PREDEFINED</definition-type>
    <id>65536</id>
  </vpn-profile>
    <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

**Sample XML Output**

```xml
<vpn-profile uri="/api/juniper/sd/vpn-management/vpn-profiles/65536">
  <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>
      </phase2-proposal>
    </custom-phase2-proposals>
  </phase2-setting>
</vpn-profile>
```
<name>Custom-proposal-1</name>
<protocol>esp</protocol>
<authentication-algorithm>sha_1</authentication-algorithm>
<encryption-algorithm>aes_cbc_128</encryption-algorithm>
<lifetime>3602</lifetime>
<lifetime>66</lifetime>
<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>
</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>
</phase2-setting>
</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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/vpn-management/vpn-profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
</tbody>
</table>
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>
                <definition-type>CUSTOM</definition-type>
            </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>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

```xml
<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/>
</vpn-profile>
```
**PUT**

This request is used to modify the VPN profile.

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

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

**Sample XML Input**

```xml
<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>
    <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>
    <auth-method>PRESHARED_KEY</auth-method>
    <phase1-proposal-type>PREDEFINED</phase1-proposal-type>
    <phase1-predefined-proposal-set>Basic</phase1-predefined-proposal-set>
    <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 is request is used to patch or to make a partial update to the VPN profile.

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

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 Phase 2 Custom Proposal**

```
<diff>
  <replace sel="vpn-profile/phase2-setting/phase2-proposal-type">
    <phase2-proposal-type>CUSTOM</phase2-proposal-type>
  </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']">
  </remove>
</diff>
```
**DELETE**

This request is used to delete the VPN profile

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/vpn-management/vpn-profiles/{profile-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP DELETE</td>
</tr>
</tbody>
</table>
| **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 Intelligence Management

- Security Intelligence RESTful Web Services on page 153
CHAPTER 12

Security Intelligence RESTful Web Services

- Security Intelligence Controller Settings Management RESTful Web Services on page 153
- Spotlight Secure Connector Management RESTful Web Services on page 157
- Security Intelligence Information Source Management RESTful Web Services on page 165
- Security Intelligence Policies Management RESTful Web Services on page 168
- Security Intelligence Profile Management RESTful Web Services on page 172
- Security Intelligence Dynamic Address Management RESTful Web Services on page 175

Security Intelligence Controller Settings Management RESTful Web Services

The following operations can be performed using the Security Intelligence Controller Settings Management RESTful Web Services. The single set of connector settings is globally applicable to all connectors.

Before creating, modifying, or fetching any connector settings, using the GET-ALL request you must determine if any connector settings already exist. If the connector settings already exist, you must first update the existing set of connector settings using the POST method, than adding any new sets. If the connector settings does not already exist, use the PUT method to update them.

GET

This request is used to collect all the security intelligence controller settings that are configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-settings-management/connector-settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.junipersd.connector-settings-management.connector-settings-refs+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of security intelligence controller settings</td>
</tr>
</tbody>
</table>
Sample Security Intelligence Controller Settings Management Output

Sample XML Output

```xml
<connector-settings
  uri="/api/juniper/sd/connector-settings-management/connector-settings" total="1">
  <connector-settings
    uri="/api/juniper/sd/connector-settings-management/connector-settings/524304"
    href="/api/juniper/sd/connector-settings-management/connector-settings/524304"
  >
    <id>524304</id>
    <name>global</name>
  </connector-settings>
</connector-settings>
```

Sample Security Intelligence Controller Settings Management Output to Get by ID

URL: /api/juniper/sd/connector-settings-management/connector-settings/{id}

Sample XML Output

```xml
<connector-settings
  uri="/api/juniper/sd/connector-settings-management/connector-settings/524304"
  href="/api/juniper/sd/connector-settings-management/connector-settings/524304"
>
  <connection-setting>
    <device-auth-token>ROS6ciuJlavzlAYcpL2m84QJgQAeVuGi</device-auth-token>
  </connection-setting>

  <email-setting>
    <port>25</port>
    <use-tls>true</use-tls>
    <enabled>true</enabled>
    <host>12</host>
    <from-address>user@example.com</from-address>
    <user-name>root</user-name>
    <password>qwe</password>
    <to-address>user@example.com</to-address>
  </email-setting>

  <upgrade-setting>
    <auto-upgrade>true</auto-upgrade>
    <hour-of-day>2</hour-of-day>
    <day-of-week>MONDAY</day-of-week>
  </upgrade-setting>

  <created-by-user-name>super</created-by-user-name>
  <id>524304</id>
  <name>global</name>

  <syslog-setting>
    <enabled>true</enabled>
    <address>asd</address>
    <verbosity>ERROR</verbosity>
  </syslog-setting>

  <last-modified-by-user-name>super</last-modified-by-user-name>
  <edit-version>1</edit-version>
</connector-settings>
```
POST

This request is for creating a new security intelligence connector setting. You must use this request if no connector settings exist in the database.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-settings-management/connector-settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-settings-management.connector-settings+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>XML payload</td>
</tr>
<tr>
<td>Produces</td>
<td>None</td>
</tr>
</tbody>
</table>

To create a new connector setting, send the new connector setting 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**

```xml
<connector-settings>
  <created-by-user-name>super</created-by-user-name>
  <name>global</name>
  <connection-setting>
    <device-auth-token>oAUZbERXrjyMssSecurityDirector</device-auth-token>
  </connection-setting>
  <email-setting>
    <port>26</port>
    <use-tls>true</use-tls>
    <enabled>true</enabled>
    <host>user</host>
    <from-address>user@example.com</from-address>
    <user-name>abc</user-name>
    <password>1234</password>
    <to-address>user@example.com</to-address>
  </email-setting>
  <upgrade-setting>
    <auto-upgrade>true</auto-upgrade>
    <repository>/tmp/cache</repository>
    <hour-of-day>2</hour-of-day>
    <day-of-week>MONDAY</day-of-week>
  </upgrade-setting>
  <syslog-setting>
    <enabled>true</enabled>
    <address>juniper</address>
    <verbosity>INFO</verbosity>
  </syslog-setting>
</connector-settings>
```

A new security intelligence connector setting is created. You can verify the same by querying Security Director to return all the connector settings.
PUT

This request is used to update the existing security intelligence connector setting.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-settings-management/connector-settings/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PUT</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-settings-management.</td>
</tr>
<tr>
<td></td>
<td>connector-settings+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>Update information</td>
</tr>
<tr>
<td>Produces</td>
<td>None</td>
</tr>
</tbody>
</table>

To modify a connector setting, send the modified information to the Junos Space server, as shown in the following example.

**Sample XML Input**

```xml
<connector-settings>
  <created-by-user-name>super</created-by-user-name>
  <id>234567</id>
  <name>global</name>
  <last-modified-by-user-name>super</last-modified-by-user-name>
  <edit-version>1</edit-version>
  <connection-setting>
    <device-auth-token>oAUXZbERXrjyMssXXXXXXXXDirector</device-auth-token>
  </connection-setting>
  <email-setting>
    <port>30</port>
    <use-tls>false</use-tls>
    <enabled>true</enabled>
    <host>XXXXXXXX</host>
    <from-address>user@example.com</from-address>
    <user-name>don</user-name>
    <password>145678</password>
    <to-address>XXXXX@example.com</to-address>
  </email-setting>
  <upgrade-setting>
    <auto-upgrade>true</auto-upgrade>
    <repository>/var/tmp/</repository>
    <hour-of-day>6</hour-of-day>
    <day-of-week>TUESDAY</day-of-week>
  </upgrade-setting>
  <syslog-setting>
    <enabled>true</enabled>
    <address>XXXXXXXX</address>
    <verbosity>DEBUG</verbosity>
  </syslog-setting>
</connector-settings>
```
Spotlight Secure Connector Management RESTful Web Services

- Connector Configuration Management RESTful Web Services on page 157
- Connector Management RESTful Web Service on page 157
- Connector Trusted CA Management RESTful Web Services on page 159
- Connector Feed Update Status Management RESTful Web Services on page 161
- Add or Modify Connector Device Association RESTful Web Service on page 163
- Device Feed Status Management RESTful Web Services on page 164
- Update Device to Connector RESTful Web Services on page 165

Connector Configuration Management RESTful Web Services

The following operation can be performed using the Security Intelligence Connector Configuration Management RESTful Web Services.

**POST**

This API initiates a request to update the configuration on each connector.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-config/update-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-config.update-config-request</td>
</tr>
<tr>
<td></td>
<td>+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>XML/JSON payload</td>
</tr>
<tr>
<td>Produces</td>
<td>Updates the security intelligence connector configuration</td>
</tr>
</tbody>
</table>

**Sample XML Input**

```xml
<update-config-request>
  <update-info-src-req/>
  <update-trusted-ca>true</update-trusted-ca>
  <update-settings>true</update-settings>
</update-config-request>
```

Connector Management RESTful Web Service

The following operations can be performed using the Security Intelligence Connector Management RESTful Web Services.

**GET**

This request is used to get all the available security intelligence connectors that are configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-management/connectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
</tbody>
</table>
Sample Security Intelligence Connector Management Output

Sample XML Output

```xml
<connectors uri="/api/juniper/sd/connector-management/connectors" total="1">
  <connector uri="/api/juniper/sd/connector-management/connectors/524289" href="/api/juniper/sd/connector-management/connectors/524289">
    <feed-status>OK</feed-status>
    <connection-state>UP</connection-state>
    <id>524289</id>
    <config-state>IN_SYNC</config-state>
    <name>connector</name>
    <domain-id>2</domain-id>
    <software-version>1.0.6.1</software-version>
    <latest-software-version>1.0.6.1</latest-software-version>
    <is-primary-string>No</is-primary-string>
    <config-state-string>In Sync</config-state-string>
    <domain-name>Global</domain-name>
    <ip>10.207.97.210</ip>
    <last-modified-by-user-name>super</last-modified-by-user-name>
  </connector>
</connectors>
```

Sample Security Intelligence Connector Management Output to Get a Single Connector by ID

URL:/api/juniper/sd/connector-management/connectors/{id}

Sample XML Output

```xml
<connector uri="/api/juniper/sd/connector-management/connectors/524289">
  <feed-status>OK</feed-status>
  <connection-state>UP</connection-state>
  <id>524289</id>
  <config-state>IN_SYNC</config-state>
  <name>connector</name>
  <domain-id>2</domain-id>
  <software-version>1.0.6.1</software-version>
  <latest-software-version>1.0.6.1</latest-software-version>
  <software-up-to-date>true</software-up-to-date>
  <is-primary-string>No</is-primary-string>
  <config-state-string>In Sync</config-state-string>
  <domain-name>Global</domain-name>
  <ip>10.207.97.210</ip>
  <last-modified-by-user-name>super</last-modified-by-user-name>
</connector>
```
Connector Trusted CA Management RESTful Web Services

The following operations can be performed using the Security Intelligence Trusted CA Management RESTful Web Services.

**GET**

This request is used to get a list of all the connector trusted CAs that are configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-trusted-ca-management.connector-trusted-ca-refs+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of connector trusted CA objects (only ID and name; no certificate data)</td>
</tr>
</tbody>
</table>

Sample Security Intelligence Connector Trusted CA Management Output

```xml
<connector-trusted-cas
uri="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas"
total="2">
<connector-trusted-ca
uri="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/524307"
href="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/524307">
  <id>524307</id>
  <name>CA Disig Root R2</name>
</connector-trusted-ca>
<connector-trusted-ca
uri="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/524310"
href="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/524310">
  <id>524310</id>
  <name>Secure Certificate Services</name>
</connector-trusted-ca>
</connector-trusted-cas>
```

Sample Security Intelligence Trusted CA Management Output to Get a Single Connector Trusted CAs by ID

URI:/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/524307

The output shows the connector trusted CA object including the certificate data.
Sample XML Output

```xml
<connector-trusted-ca
  url="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/524307"
  href="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/524307"
>
  <created-by-user-name>super</created-by-user-name>
  <edit-version>1</edit-version>
  <domain-name>Global</domain-name>
  <version>0</version>
  <id>524307</id>
  <last-modified-by-user-name>super</last-modified-by-user-name>
  <trusted-ca-cert>
    -----BEGIN CERTIFICATE-----
    MIIFaTCCA1GgAwIBAgIJAJK4iNuwisFjMA0GCSqGSIb3DQEBCwUAMFIxCzAJBgNVBAYTAlNLMRMwUxLMVYdh84uEEZhvUQh0m9dM9+JDX6HAcOmw0Ly8xL4ysEr3vQCJ8KWeqshNPZITEUxnhpIkV7+ZtsH8tZ/3zbBtIRqPIShfpNC
    -----END CERTIFICATE-----
  </trusted-ca-cert>
  <domain-id>2</domain-id>
  <name>CADisigRootR2</name>
</connector-trusted-ca>
```

**POST**

This request adds a new connector trusted CA.

**URI**

/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/URI

**HTTP Method**

HTTP POST

**Content-Type**

application/vnd.juniper.sd.connector-trusted-ca-management.connector-trusted-ca+xml;version=1;charset=UTF-8

**Sample XML Input**

```xml
<connector-trusted-ca
  <name>CADisigRootR2</name>
  <definition-type>CUSTOM</definition-type>
  <trusted-ca-cert>
    -----BEGIN CERTIFICATE-----
    MIIFaTCCA1GgAwIBAgIJAJK4iNuwisFjMA0GCSqGSIb3DQEBCwUAMFIxCzAJBgNVBAYTAlNLMRMwUxLMVYdh84uEEZhvUQh0m9dM9+JDX6HAcOmw0Ly8xL4ysEr3vQCJ8KWeqshNPZITEUxnhpIkV7+ZtsH8tZ/3zbBtIRqPIShfpNC
    -----END CERTIFICATE-----
  </trusted-ca-cert>
</connector-trusted-ca>
```
**DELETE**

This request deletes the connector trusted CA by ID.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>text/plain; charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>None</td>
</tr>
</tbody>
</table>

**DELETE (Many)**

This request deletes one or more connector trusted CAs by ID.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-trusted-ca-management.delete-many-request+xml;version=1; charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>Collection of connector trusted CA objects by ID only (no certificate data)</td>
</tr>
<tr>
<td>Produces</td>
<td>None</td>
</tr>
</tbody>
</table>

**Sample XML Input**

```
<delete-many-request uri="/api/juniper/sd/connector-trusted-ca-management/connector-trusted-cas">
  <ids>
    <id>Integer</id>
  </ids>
</delete-many-request>
```

**Connector Feed Update Status Management**

**RESTful Web Services**

The following operations can be performed using the Security Intelligence Connector Management RESTful Web Services. A connector can have several feeds. This API returns a collection of status objects.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-management/connectors/[id]/connector-feed-update-status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-management.connector-feed-update-statuses+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
</tbody>
</table>
Consumes
None

Produces
Collection of connector feed update statuses

Sample Security Intelligence Connector Feed Update Status Output

Sample XML Output

```xml
<connector-feed-update-statuses total="8">
  <connector-feed-update-status>
    <connector-id>524289</connector-id>
    <category>IPFILTER</category>
    <feed-name>IFServer</feed-name>
    <last-update-time>2015-01-29T05:05:19Z</last-update-time>
    <success>true</success>
  </connector-feed-update-status>

  <connector-feed-update-status>
    <connector-id>524289</connector-id>
    <category>GEOIP</category>
    <feed-name>geoip_country</feed-name>
    <last-update-time>2015-01-28T06:03:06Z</last-update-time>
    <success>true</success>
  </connector-feed-update-status>

  <connector-feed-update-status>
    <connector-id>524289</connector-id>
    <category>CC</category>
    <feed-name>cc_ip_data</feed-name>
    <last-update-time>2015-01-29T05:35:14Z</last-update-time>
    <success>true</success>
  </connector-feed-update-status>

  <connector-feed-update-status>
    <connector-id>524289</connector-id>
    <category>CC</category>
    <feed-name>cc_url_data</feed-name>
    <last-update-time>2015-01-29T05:34:32Z</last-update-time>
    <success>true</success>
  </connector-feed-update-status>

  <connector-feed-update-status>
    <connector-id>524289</connector-id>
    <category>IPFILTER</category>
    <feed-name>IFFileUpload</feed-name>
    <last-update-time>2015-01-29T05:50:11Z</last-update-time>
    <success>true</success>
  </connector-feed-update-status>

  <connector-feed-update-status>
    <connector-id>524289</connector-id>
    <category>WHITELIST</category>
    <feed-name>IFFileUpload</feed-name>
    <last-update-time>2015-01-29T05:58:41Z</last-update-time>
    <success>true</success>
  </connector-feed-update-status>
</connector-feed-update-statuses>
```
Connector Feed Update Status Summary

The following operations can be performed using the Security Intelligence Connector Management RESTful Web Services. This request is used to collect all the connector feed update status summary.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-management/connectors/{id}/connector-feed-update-status-summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-management.connector-feed-update-statuses+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of connector feed update status summary</td>
</tr>
</tbody>
</table>

Sample Output of to Get Connector Feed Update Status Summary by ID

```xml
<connector uri="/api/juniper/sd/connector-management/connectors/524289/connector-feed-update-status-summary">
  <feed-status>OK</feed-status>
  <connection-state>UP</connection-state>
  <ha>false</ha>
  <id>524289</id>
  <config-state>IN_SYNC</config-state>
  <name>connector</name>
  <is-primary-string>No</is-primary-string>
  <ha-members/>
  <is-primary>false</is-primary>
  <ha-string>No</ha-string>
  <config-state-string>In Sync</config-state-string>
  <domain-id>2</domain-id>
  <software-version>1.0.6.1</software-version>
  <edit-version>8</edit-version>
  <software-up-to-date>true</software-up-to-date>
  <domain-name>Global</domain-name>
  <ip>10.207.97.210</ip>
  <last-modified-by-user-name>super</last-modified-by-user-name>
  <latest-software-version>1.0.6.1</latest-software-version>
  <num-associated-devices>0</num-associated-devices>
  <ha-members-string/>
  <mgmt-ip>10.207.97.210</mgmt-ip>
  <definition-type>CUSTOM</definition-type>
</connector>
```

Add or Modify Connector Device Association RESTful Web Service

The following operations can be performed using the Security Intelligence Connector Management RESTful Web Services.
### POST

This request handles associating and dissociating devices from a connector.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-management/connectors/{id}/associate-devices-to-connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-management.associate-devices-to-connector-request+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>Collections of devices to add or delete</td>
</tr>
</tbody>
</table>

**Sample XML Input**

```xml
<associate-devices-to-connector-request>
  <add-device-list>
    <add-device>deviceID</add-device>
  </add-device-list>
  <delete-device-list>
    <delete-device>deviceID</delete-device>
  </delete-device-list>
</associate-devices-to-connector-request>
```

### Device Feed Status Management RESTful Web Services

The following operation can be performed using the Security Intelligence Connector Management RESTful Web Services.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/connector-management/connectors/{id}/device-feed-status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.connector-management.device-feed-status+xml;version=1;q=0.01</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of device update statuses</td>
</tr>
</tbody>
</table>

**Sample Output to Get Device Feed Status by ID**

```xml
<device-feed-status-list>
  <device-feed-status>
    <device-name>10.205.255.38-Secintel</device-name>
    <connector-connection-status>UP</connector-connection-status>
    <feed-status>OK</feed-status>
    <device-ip>10.205.255.38</device-ip>
  </device-feed-status>
</device-feed-status-list>
```
Update Device to Connector RESTful Web Services

The following operation can be performed using the Security Intelligence Device Management RESTful Web Services. This request updates the devices to the spotlight secure connector after you associate these devices to the connectors.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/device-management/update-connector-settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.device-management.update-connector-settings+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>Collection of devices to update</td>
</tr>
<tr>
<td>Produces</td>
<td>None</td>
</tr>
</tbody>
</table>

Sample XML Input

```xml
<update-connector-settings>
  <set-device-ids>
    <device-id>device-id</device-id>
  </set-device-ids>
  <connector-id>connector-id</connector-id>
</update-connector-settings>
```

Security Intelligence Information Source Management RESTful Web Services

The following operations can be performed using the Security Intelligence Information Source Management RESTful Web Services.

GET

This request is used to collect all the security intelligence information sources that are configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/info-source-management/info-sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.info-source-management.info-source-refs+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of security intelligence information sources</td>
</tr>
</tbody>
</table>

Sample Security Intelligence Information Source Management Output

```xml
<info-sources uri="/api/juniper/sd/info-source-management/info-sources" total="4">
  <info-source href="/api/juniper/sd/info-source-management/info-sources/524292">
    <description>source2</description>
  </info-source>
</info-sources>
```
Sample Security Intelligence Information Source Management Output to Get Information Sources by ID

URL: /api/juniper/sd/info-source-management/info-sources/{info-source-id}

Sample XML Output

```xml
<info-source href="/api/juniper/sd/info-source-management/info-sources/524295"/>
<id>524295</id>
<description/>
<upload-file-name>blacklist-new1.txt</upload-file-name>
<created-by-user-name>super</created-by-user-name>
<last-modified-by-user-name>super</last-modified-by-user-name>
<edit-version>1</edit-version>
<update-interval>NEVER</update-interval>
<name>IFFileUpload</name>
<source>CUSTOM_FILE</source>
<encoding>IPRECORD</encoding>
</info-source>
```

**POST**

This request is for creating a new security intelligence information source.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/info-source-management/info-sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
</tbody>
</table>
To create a new information source, send the new information source 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**

```xml
<info-source>
  <description>File Server</description>
  <password>juniper</password>
  <update-interval>HOURLY</update-interval>
  <name>test5</name>
  <address>http://10.205.31.25/SD-Laptop.txt</address>
  <source>CUSTOM_SERVER</source>
  <user-name>user</user-name>
  <encoding>IPRECORD</encoding>
</info-source>

<info-source>
  <description>CLOUD</description>
  <name>test6</name>
  <source>CLOUD</source>
</info-source>
```

A new security intelligence information source is created. You can verify the same by querying Security Director to return all the information sources.

**PUT**

This request is used to modify a security intelligence information source.

**URI**

api/juniper/sd/info-source-management/info-sources/{id}

**HTTP Method**

HTTP PUT

**Content-Type**

application/vnd.juniper.sd.info-source-management.info-source+xml;version=1;charset=UTF-8

**Consumes**

None
Modifies a security intelligence information source

To modify an information source, send the modified information to the Junos Space server, as shown in the following example.

Sample XML Input 1

```xml
<info-source>
  <id>3423</id>
  <edit-version>1</edit-version>
  <description>File Server modify</description>
  <password>juniper123</password>
  <update-interval>DAILY</update-interval>
  <name>test5</name>
  <address>http://10.205.31.25/SD-Laptop.txt</address>
  <source>CUSTOM_SERVER</source>
  <user-name>modify</user-name>
  <encoding>IPRECORD</encoding>
</info-source>
```

Sample XML Input 2

```xml
<info-source>
  <id>4567</id>
  <edit-version>1</edit-version>
  <description>CLOUD modify</description>
  <name>test6_modify</name>
  <source>CLOUD</source>
</info-source>
```

DELETE

This request deletes the security intelligence information source by ID.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/info-source-management/info-sources/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.info-source-management.info-source+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes an information source</td>
</tr>
</tbody>
</table>

Security Intelligence Policies Management RESTful Web Services

The following operations can be performed using the Security Intelligence Management RESTful Web Services.
GET

This request collects all the security intelligence policies that are configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/secintel-management/secintel-policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.secintel-management.secintel-policies+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of security intelligence policies</td>
</tr>
</tbody>
</table>

Sample Security Intelligence Profiles Management Output

```xml
<secintel-policies uri="/api/juniper/sd/secintel-management/secintel-policies" total="2">
  <secintel-policy uri="/api/juniper/sd/secintel-management/secintel-policies/295932" href="/api/juniper/sd/secintel-management/secintel-policies/295932" edit-version="1">
    <created-by-user-name>super</created-by-user-name>
    <domain-name>Global</domain-name>
    <id>295932</id>
    <description/>
    <name>Policy1</name>
    <domain-id>2</domain-id>
    <secintel-profiles>
      <secintel-profile>
        <block-threshold-type>RECOMMENDED</block-threshold-type>
        <block-threshold-level>8</block-threshold-level>
        <block-option>DROP_CONNECTION_SILENTLY</block-option>
        <log-option>LOG_ALL</log-option>
        <description>source</description>
        <category>CommandAndControl</category>
        <domain-name>Global</domain-name>
        <id>295929</id>
        <name>Control1</name>
      </secintel-profile>
    </secintel-profiles>
  </secintel-policy>
  <secintel-policy uri="/api/juniper/sd/secintel-management/secintel-policies/295933" href="/api/juniper/sd/secintel-management/secintel-policies/295933" edit-version="2">
    <created-by-user-name>super</created-by-user-name>
    <domain-name>Global</domain-name>
    <id>295933</id>
  </secintel-policy>
</secintel-policies>
```
<description>Policy</description>
<name>Policy2</name>
<domain-id>2</domain-id>

<secintel-profiles>
<secintel-profile>
<block-threshold-type>NONE</block-threshold-type>
<description/>
<category>CommandAndControl</category>
<domain-name>Global</domain-name>
<id>295931</id>
<name>Control3</name>
</secintel-profile>
</secintel-profiles>
</secintel-policy>
</secintel-policies>

Sample Security Intelligence Policies Management Output to Get Policies by ID

URI:/api/juniper/sd/secintel-management/secintel-policies/{policy-id}

Sample XML Output

<secintel-policy uri="/api/juniper/sd/secintel-management/secintel-policies/295933">
<edit-version>2</edit-version>
<created-by-user-name>super</created-by-user-name>

<secintel-profiles>
<secintel-profile>
<block-threshold-type>NONE</block-threshold-type>
<description/>
<category>CommandAndControl</category>
<domain-name>Global</domain-name>
<id>295931</id>
<name>Control3</name>
</secintel-profile>
</secintel-profiles>
<domain-name>Global</domain-name>
<id>295933</id>
<description>Policy</description>
<name>Policy2</name>
<domain-id>2</domain-id>
</secintel-policy>

POST

This request is for creating a new security intelligence policy.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/secintel-management/secintel-policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.secintel-management.secintel-policy+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
</tbody>
</table>
To create a new policy, send the new policy 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**

```
<secintel-policy>
  <name>Secintelpolicy-1</name>
  <description>Description of policy 1</description>
  <secintel-profiles>
    <secintel-profile>
      <id>0000secintel-profiles-secintel-profile1</id>
      <name>secinte-profile1</name>
    </secintel-profile>
  </secintel-profiles>
</secintel-policy>
```

**Sample XML Input 2**

```
<secintel-policy>
  <name>Secintelpolicy-2</name>
  <description>Description of policy 2</description>
  <secintel-profiles>
    <secintel-profile>
      <id>0000secintel-profiles-secintel-profile2</id>
      <name>secinte-profile2</name>
    </secintel-profile>
  </secintel-profiles>
</secintel-policy>
```

A new security intelligence policy is created. You can verify the same by querying Security Director to return all the policies.

**PUT**

This request is used to modify a security intelligence policy.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/secintel-management/secintel-policies/{policy-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PUT</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.secintel-management.secintel-policy+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Modifies a security intelligence policy</td>
</tr>
</tbody>
</table>

To modify a policy, send the modified information to the Junos Space server, as shown in the following example.

**Sample XML Input**

```
<secintel-policy>
  <name>Secintelpolicy-1</name>
  <description>Modified Description of policy 1</description>
</secintel-policy>
```
<id>0000secintel-policies-Secintelpolicy-1</id>
<edit-version>1</edit-version>
<secintel-profiles>
<secintel-profile>
<id>0000secintel-profiles-secintel-profile2</id>
<name>secinte-profile2</name>
</secintel-profile>
</secintel-profiles>

Sample XML Input 2

<secintel-policy>
<name>Secintelpolicy-2</name>
<description>Modified Description of policy 2</description>
<id>0000secintel-policies-Secintelpolicy-2</id>
<edit-version>1</edit-version>
<secintel-profiles>
<secintel-profile>
<id>0000secintel-profiles-secintel-profile1</id>
<name>secinte-profile1</name>
</secintel-profile>
</secintel-profiles>
</secintel-policy>

DELETE

This request deletes the security intelligence policies by ID.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/secintel-management/secintel-policies/{policy-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.secintel-management.secintel-policy+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes a policy</td>
</tr>
</tbody>
</table>

Security Intelligence Profile Management RESTful Web Services

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

GET

This request is used to collect all the security intelligence profiles that are configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/secintel-management/secintel-profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
</tbody>
</table>
Sample Security Intelligence Profiles Management Output

**Sample XML Output**
```
<secintel-profiles uri="/api/juniper/sd/secintel-management/secintel-profiles" total="6">
  <secintel-profile uri="/api/juniper/sd/secintel-management/secintel-profiles/295925" href="/api/juniper/sd/secintel-management/secintel-profiles/295925">
    <domain-name>Global</domain-name>
    <id>295925</id>
    <category>CommandAndControl</category>
    <block-threshold-type>RECOMMENDED</block-threshold-type>
    <block-threshold-level>6</block-threshold-level>
    <block-option>CLOSE_SERVER_CLIENT_CONN</block-option>
    <log-option>LOG_ALL</log-option>
    <name>FingerPrintProfile1</name>
  </secintel-profile>
  <secintel-profile uri="/api/juniper/sd/secintel-management/secintel-profiles/295926" href="/api/juniper/sd/secintel-management/secintel-profiles/295926">
    <domain-name>Global</domain-name>
    <id>295926</id>
    <category>CommandAndControl</category>
    <block-threshold-type>NONE</block-threshold-type>
    <description/>
    <name>FingerPrintProfile2</name>
  </secintel-profile>
</secintel-profiles>
```

Sample Security Intelligence Profiles Management Output to Get Profiles by ID

**Sample XML Output**
```
<secintel-profile uri="/api/juniper/sd/secintel-management/secintel-profiles/295930">
  <created-by-user-name>super</created-by-user-name>
  <edit-version>1</edit-version>
  <domain-name>Global</domain-name>
  <id>295930</id>
  <category>CommandAndControl</category>
  <block-threshold-type>CUSTOM</block-threshold-type>
  <redirect-message>http://example.com</redirect-message>
  <block-threshold-level>9</block-threshold-level>
  <block-option>CLOSE_SERVER_CLIENT_CONN</block-option>
  <log-option>NO_LOG</log-option>
  <directory/>
  <name>Control2</name>
</secintel-profile>
```
**POST**

This request is for creating a new security intelligence profile.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/secintel-management/secintel-profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP POST</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.secintel-management.secintel-profile+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td><strong>Consumes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Produces</strong></td>
<td>Creates a new security intelligence profile</td>
</tr>
</tbody>
</table>

To create a new profile, send the new profile 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**

```xml
<secintel-profile>
  <category>CommandAndControl</category>
  <block-threshold-type>CUSTOM</block-threshold-type>
  <redirect-message />
  <block-threshold-level>7</block-threshold-level>
  <block-option>CLOSE_SERVER_CLIENT_CONN</block-option>
  <log-option>LOG_BLOCKED</log-option>
  <redirect-message-type>NONE</redirect-message-type>
  <description>Profile-8</description>
  <name>secintel-profile8</name>
</secintel-profile>
```

A new security intelligence profile is created. You can verify the same by querying Security Director to return all the profiles.

**PUT**

This request is used to modify a security intelligence profile.

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/secintel-management/secintel-profiles/{profile-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP PUT</td>
</tr>
<tr>
<td><strong>Content-Type</strong></td>
<td>application/vnd.juniper.sd.secintel-management.secintel-profile+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td><strong>Consumes</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Produces</strong></td>
<td>Modifies a security intelligence profile</td>
</tr>
</tbody>
</table>

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

**Sample XML Input**

```xml
<secintel-profile>
  <category>CommandAndControl</category>
  ...
</secintel-profile>
```
DELETE

This request deletes the security intelligence profiles by ID.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/secintel-management/secintel-profiles/{profile-id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.secintel-management.secintel-profile+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Deletes a profile</td>
</tr>
</tbody>
</table>

Security Intelligence Dynamic Address Management RESTful Web Services

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

GET

This request is used to collect all the security intelligence dynamic addresses that are configured in Security Director.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/dynamic-address-management/dynamic-addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.dynamic-address-management. dynamic-address-refs+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of security intelligence dynamic addresses</td>
</tr>
</tbody>
</table>

Sample Security Intelligence Dynamic Address Management Output

Sample XML Output

```xml
<dynamic-addresses
  href="/api/juniper/sd/dynamic-address-management/dynamic-addresses" total="3"
  url="/api/juniper/sd/dynamic-address-management/dynamic-addresses"
>```

Copyright © 2016, Juniper Networks, Inc.
<dynamic-address
url="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295924"
href="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295924"
>
  <id>295924</id>
  <domain-id>2</domain-id>
  <name>DAG1</name>
  <domain-name>Global</domain-name>
</dynamic-address>

<dynamic-address
url="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295935"
href="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295935"
>
  <id>295935</id>
  <domain-id>2</domain-id>
  <name>DAG2</name>
  <domain-name>Global</domain-name>
</dynamic-address>

<dynamic-address
url="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295937"
href="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295937"
>
  <id>295937</id>
  <domain-id>2</domain-id>
  <name>DAG3</name>
  <domain-name>Global</domain-name>
</dynamic-address>

Sample Security Intelligence Dynamic Address Management Output to Get by ID

URL: api/juniper/sd/dynamic-address-management/dynamic-addresses/295924

Sample XML Ouput

```
<dynamic-address
url="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295924"
href="/api/juniper/sd/dynamic-address-management/dynamic-addresses/295924"
>
  <created-by-user-name>super</created-by-user-name>
  <countries>
    <country>
      <code>AF</code>
      <display-name>Afghanistan</display-name>
    </country>
    <country>
      <code>BE</code>
      <display-name>Belgium</display-name>
    </country>
  </countries>
  <negate-selected-countries>false</negate-selected-countries>
  <id>295924</id>
  <description/>
  <domain-id>2</domain-id>
  <name>DAG1</name>
```

```
POST

This request is for creating a new security intelligence dynamic address.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/dynamic-address-management/dynamic-addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.dynamic-address-management. dynamic-address+xml;version=1;charset=UTF-8</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Creates a new security intelligence dynamic address</td>
</tr>
</tbody>
</table>

To create a new dynamic address, send the new dynamic address 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**

```xml
<dynamic-address>
  <name>Dynamic-add1</name>
  <category>GEO_IP</category>
  <feedName>GeoIP</feedName>
  <description>Desc of Dynamic address1</description>
  <countries>
    <country>
      <code>CN</code>
      <display-name>China</display-name>
    </country>
    <country>
      <code>AE</code>
      <display-name>United Arab Emirates</display-name>
    </country>
  </countries>
</dynamic-address>
```

PUT

This request is used to modify a security intelligence dynamic address.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/dynamic-address-management/dynamic-addresses/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP PUT</td>
</tr>
</tbody>
</table>

Copyright © 2016, Juniper Networks, Inc.
To modify a dynamic address, send the modified information to the Junos Space server, as shown in the following example.

**Sample XML Input**

```xml
<dynamic-address>
  <name>Dynamic-add1</name>
  <id>234561</id>
  <edit-version>1</edit-version>
  <category>GEO_IP</category>
  <feedName>GeoIP</feedName>
  <negate-selected-countries>true</negate-selected-countries>
  <description>Desc of Dynamic address1 modified</description>
  <countries>
    <country>
      <code>AQ</code>
      <display-name>Antarctica</display-name>
    </country>
    <country>
      <code>IN</code>
      <display-name>India</display-name>
    </country>
  </countries>
</dynamic-address>
```

**DELETE**

This request deletes the security intelligence dynamic address by ID.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/dynamic-address-management/dynamic-addresses/{id}</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP DELETE</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.dynamic-address-management.</td>
</tr>
<tr>
<td></td>
<td>dynamic-address+xml;version=1; charset=UTF-8</td>
</tr>
</tbody>
</table>

| Consumes             | None                                                          |
| Produces             | Deletes the dynamic address                                   |
PART 5

Security Device Management

- Device Management RESTful Web Services on page 181
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.

<table>
<thead>
<tr>
<th>URI</th>
<th>/api/juniper/sd/device-management/devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>application/vnd.juniper.sd.device-management.devices+xml;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td></td>
<td>application/vnd.juniper.sd.device-management.devices+json;q=&quot;0.01&quot;;version=&quot;1&quot;</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Collection of device information</td>
</tr>
</tbody>
</table>

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 url="/api/juniper/sd/device-management/devices" total="1">
  <device url="/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>
  </device>
</devices>
```
Sample Device Management Input and Output to Get Device by ID

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

**Sample XML Output**
```xml
<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>
  <Zonerel="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**
```xml
<zones total="5" url="/api/juniper/sd/device-management/devices/426240/zones">
  <zone>
    <name>trust</name>
    <interfaces total="0">
      <interface>ge-0/0/0.0</interface>
    </interfaces>
  </zone>
  ...  // Other zones...
</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

```xml
<interfaces total="4"
url="/api/juniper/sd/device-management/devices/98939/interfaces"/>
<interface>
<cems-moid>net.juniperjmpa.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>
```
<name>ge-0/0/0.0</name>
</interface>

<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>198.51.100.0</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/>
  <unit>0</unit>
  <id>327692</id>
  <name>ge-0/0/1.0</name>
</interface>

<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>198.51.100.1</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/>
  <unit>0</unit>
  <id>327694</id>
  <name>ge-0/0/2.0</name>
</interface>
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"
  url="/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.

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/device-management/update-devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP POST</td>
</tr>
</tbody>
</table>
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(000130))

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.
### Sample Input Request to Collect All the Certificates of the Devices

<table>
<thead>
<tr>
<th><strong>URI</strong></th>
<th>/api/juniper/sd/device-management/devices-certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method</strong></td>
<td>HTTP POST</td>
</tr>
</tbody>
</table>
| **Content-Type** | application/vnd.juniper.sd.device-management.certificates-request+xml;version=2;charset=UTF-8  
application/vnd.juniper.sd.device-management.certificates+xml;version=1;q=0.01  
application/vnd.juniper.sd.device-management.certificates-request+json;version=2;charset=UTF-8  
application/vnd.juniper.sd.device-management.certificates+json;version=1;q=0.01 |
| **Consumes** | None |
| **Produces** | List of certificates |

To get the list of certificates, send the query to the Junos Space server, as shown in the following example.

**Sample XML Input**

```
<certificates-for-devices-request>
  <device-id-list>
    <ids>Integer</ids>
  </device-id-list>
  <auth-method>PRESHARED_KEY</auth-method>
</certificates-for-devices-request>
```

**Related Documentation**
- Security Director RESTful Web Services Overview on page 3
- Using Security Director RESTful Web Services on page 5
PART 6

Security Director Job Management

- Job Management RESTful Web Services on page 191
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.

---

<table>
<thead>
<tr>
<th>URI</th>
<th>api/juniper/sd/job-management/jobs/[job-id]/device-results</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Method</td>
<td>HTTP GET</td>
</tr>
<tr>
<td>Content-Type</td>
<td>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</td>
</tr>
<tr>
<td>Consumes</td>
<td>None</td>
</tr>
<tr>
<td>Produces</td>
<td>Returns the device specific status for a particular update job.</td>
</tr>
</tbody>
</table>

Sample XML Output

```
<device-results total="1"
  url="/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>10.205.119.25</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

```xml
<configuration total="1"
url="/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>
            </gateway>
          </ike>
        </security>
      </configuration>
    </edit-config>
  </configuration>
</configuration>
```

Copyright © 2016, Juniper Networks, Inc.
<!--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>
<policyoperation="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>
<policyoperation="create">
<name>testVPN</name>
<proposal-set>standard</proposal-set>
</policy>
<vpnoperation="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>
</ike>
</vpn>
</ipsec>
<policies>
<policy>
<from-zone-name>trust</from-zone-name>
<to-zone-name>untrust</to-zone-name>
<policyoperation="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>
<policyoperation="create">
<name>Device-Zone-3</name>
<match>
<application>any</application>
<destination-address>ad1</destination-address>
</policy>
</policies>
<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>192.0.2.6/24</ip-prefix>
         </address>
      </address-book>
   </security-zone>
</zones>
<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>VPN</name>
  <interfaces operation="create">
    <name>st0.2</name>
  </interfaces>
</security-zone>
</zones>
</security>
</configuration>

Related Documentation
• Security Director RESTful Web Services Overview on page 3
• Using Security Director RESTful Web Services on page 5