



SMC Web Services Programming Guide

October 30, 2018

Table of Contents

1	Introduction.....	5
1.1	About this document	5
1.2	Prerequisites	5
1.3	Additional Documentation	5
2	Overview	6
2.1	SOAP	6
2.2	Transport	6
2.3	Authentication & Access Control	6
2.4	Addressing.....	6
2.5	Example	7
2.6	Filter Semantics.....	8
2.7	Identifiers.....	8
2.8	Building Web Service Requests from the SMC GUI.....	9
3	Reference.....	11
3.1	getDSCPTraffic	11
3.1.1	Request	11
3.1.2	Response.....	12
3.2	getFlows	13
3.2.1	Request	13
3.2.2	Response.....	21
3.3	getSecurityEvents.....	27
NOTE: 'getCiEvents' is deprecated and has been replaced with 'getSecurityEvents' in version		
v6.5.	The 'getCiEvents' service will not be supported in future releases.....	27
3.3.1	Request	27
3.3.2	Response.....	29
3.4	getHostSnapshot.....	31
3.4.1	Request	31
3.4.2	Response.....	32
3.5	getHostInformation.....	49
3.5.1	Request	49
3.5.2	Response.....	53
3.6	getHostGroups.....	58
3.6.1	Request	58
3.6.2	Response.....	58
3.7	setHostGroups.....	59
3.7.1	Request	59
3.7.2	Response.....	60
3.8	updateExporters.....	60
3.8.1	Request	60
3.8.2	Response.....	63
3.9	removeExporters.....	63
3.9.1	Request	63
3.9.2	Response.....	64
3.10	updateExporterSNMPConfiguration.....	64
3.10.1	Request.....	64
3.10.2	Response	66
3.11	addHostGroup	66
3.11.1	Request.....	66
3.11.2	Response	67
3.12	addHostGroups.....	67
3.12.1	Request.....	68
3.12.2	Response	69
3.13	addHostGroupIPRange	69

3.13.1	Request.....	69
3.13.2	Response.....	69
3.14	addHostGroupIPRanges.....	69
3.14.1	Request.....	70
3.14.2	Response.....	70
3.15	removeHostGroup.....	70
3.15.1	Request.....	70
3.15.2	Response.....	71
3.16	removeHostGroupIPRange.....	71
3.16.1	Request.....	71
3.16.2	Response.....	71
3.17	setHostGroupIPRange.....	71
3.17.1	Request.....	71
3.17.2	Response.....	72
3.18	getDomain.....	72
3.18.1	Request.....	72
3.18.2	Response.....	72
3.19	addDomain.....	72
3.19.1	Request.....	72
3.19.2	Response.....	76
3.20	removeDomain.....	77
3.20.1	Request.....	77
3.20.2	Response.....	77
4	Appendix.....	78
4.1	Date & Time Filtering.....	78
4.1.1	Time Range Selection.....	78
4.1.2	Time Window Selection.....	78
4.1.3	Day Selection.....	79
4.1.4	Day Range Selection.....	79
4.1.5	Active Time Selection.....	79
4.1.6	First-Last Time Selection.....	80
4.2	Device Filtering.....	81
4.2.1	Device List Selection.....	81
4.2.2	Exporter Selection.....	81
4.2.3	Interface Selection.....	81
4.3	Host Filtering.....	82
4.3.1	Host Group Selection.....	82
4.3.2	IP Address Range Selection.....	82
4.3.3	IP Address List Selection.....	82
4.3.4	IP Address Selection.....	83
4.3.5	VM Selection.....	83
4.3.6	Host Pair Selection.....	83
4.4	Service Profile Status.....	84
4.5	Alarm Types.....	85
4.6	Security Event Types.....	89
4.6.1	In previous versions, these were known as CI Events.....	89
4.7	ICMP Types.....	91
5	Examples of Accessing SMC Web Services.....	93
5.1	Using 'wget'.....	93
5.1.1	'getDomain' request example.....	93
5.1.2	'getHostSnapshot' request.....	93
5.2	Using 'curl'.....	94
5.2.1	'getHostInformation' request.....	94
5.2.2	'getSecurityEvents' request.....	94
5.3	Using 'python'.....	95
5.3.1	'addDomain' request.....	95

1 Introduction

1.1 About this document

This document aims to explain the operation of the StealthWatch Management Console (SMC) Web Service that is present in this version of the SMC product. This guide supports Stealthwatch Enterprise v6.10.x and v7.0.x.

1.2 Prerequisites

It is assumed that the reader is familiar with the following concepts:

- Extensible Markup Language (XML)
- XML Schema Definition (XSD)
- Web Services Description Language (WSDL) version 1.1
- Simple Object Access Protocol (SOAP) version 1.2

1.3 Additional Documentation

While this document serves as a guide to users of the SMC Web Service, the following documents provide the full formal specification of the SMC Web Service:

- SMC Web Service WSDL Definition (`sws.wsdl`)
- SMC Web Service XML Message Types (`sws-message.xsd`)
- SMC XML Data Record Types (`sws-record.xsd`)
- SMC XML Types (`sws.xsd`)

There is the server-side and the client-side version of these documents. A client should be initialized with **the client-side version** of the documents. All of the files are located in the following two files. The URL for each file is included.

- Web Services API Schema - Client

https://lancope.my.salesforce.com/sfc/p/#300000000QWy/a/380000008snFV/hoOCKF_Db3TjxE.B.XS2rvc1toedYYFPr41BUUmoxM4

- Web Services - Server

<https://lancope.my.salesforce.com/sfc/p/#300000000QWy/a/380000008stX/LN3Y1NhzFsFBzM78pBnyGolnpEDFM62zbDIdkFkOOw>

2 Overview

2.1 SOAP

The SMC Web Service uses a single type of binding for service endpoints, or ports, that use the SOAP to transfer XML payloads between the client and the server. The encoding that is used for the XML payload within the SOAP messages is constrained in the following ways:

- The input message has a single part (`soap:body` has only one child)
- The part is an element
- The element has the same name as the operation
- The element's complex type has no attributes

This style of SOAP-WSDL binding is often termed “document/literal wrapped” and is illustrated in the proceeding examples.

2.2 Transport

The SMC Web Service uses *HTTPS* (HTTP with TLS) as the transport for the SOAP messages.

2.3 Authentication & Access Control

The SMC Web Service delegates authentication of the client to the HTTP transport. Specifically, the SMC Web Service utilizes *HTTP Basic Authentication*. The client should use credentials that have been set up on the SMC through the SMC Web Start Client.

Access to data and operations through the SMC Web Service is then restricted by the Data Role and Function Roles assigned to that user.

Please refer to the *SMC Online Help* for instructions on creating and managing SMC users and roles.

2.4 Addressing

The SMC Web Service WSDL describes the HTTP address for the ports in the following fashion:

```
<wsdl:port name="flowsPort" binding="tns:flowsBinding">
  <soap:address location="http://WWW.LANCOPE.COM/smc/swsService/flows" />
</wsdl:port>
```

When addressing this service port in the real world there are two things to note:

1. While the URLs in the WSDL specify the HTTP protocol the SMC Web Service actually uses HTTPS.
2. The URLs in the WSDL specify WWW.LANCOPE.COM as the host. This should be substituted with the IP address or host name of the SMC.

For example, to access the service port defined above for an SMC at 192.168.1.100, the actual URL that the client would use would be:

<https://192.168.1.100/smc/swsService/flows>

2.5 Example

Let us say that the client would like to access the `getFlows` operation in the `flowsPort` service port. The pertinent part of the WSDL would be:

```
<wsdl:message name="getFlowsRequest">
  <wsdl:part name="parameters" element="getFlows" />
</wsdl:message>

<wsdl:message name="getFlowsResponse">
  <wsdl:part name="parameters" element="getFlowsResponse" />
</wsdl:message>

<wsdl:portType name="flows">
  <wsdl:operation name="getFlows">
    <wsdl:input message="tns:getFlowsRequest" />
    <wsdl:output message="tns:getFlowsResponse" />
  </wsdl:operation>
  :
  :
</wsdl:portType>

<wsdl:binding name="flowsBinding" type="tns:flows">
  <soap:binding style="document"
    transport="http://schemas.xmlsoap.org/soap/http" />
  <wsdl:operation name="getFlows">
    <wsdl:input>
      <soap:body use="literal" />
    </wsdl:input>
    <wsdl:output>
      <soap:body use="literal" />
    </wsdl:output>
  </wsdl:operation>
  :
  :
</wsdl:binding>
<wsdl:service name="swsService">
  <wsdl:port name="flowsPort" binding="tns:flowsBinding">
    <soap:address
      location="http://WWW.LANCOPE.COM/smc/swsService/flows" />
  </wsdl:port>
  :
  :
wsdl:service>
```

The URL to HTTP POST the request to would be:

<https://192.168.1.100/smc/swsService/flows>

The request would be:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getFlows>
      :
      <!--request payload XML -->
      :
    </getFlows>
  </soapenc:Body>
</soapenc:Envelope>
```

The response would be:

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenc:Envelope xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getFlowsResponse>
      :
      <!--response payload XML -->
      :
    </getFlowsResponse>
  </soapenc:Body>
</soapenc:Envelope>
```

2.6 Filter Semantics

The request XML payload to the SMC Web Service is termed a filter and contains a description of the constraints to be placed on the returned results.

It is important to note that, in general the contents of the filters are interpreted through AND logic: the returned results must satisfy ALL of the supplied constraints.

However, in certain cases some sub-set of constraints may follow OR logic: the returned results must satisfy AT LEAST ONE of the supplied constraints. These cases will be highlighted in the proceeding reference section.

2.7 Identifiers

The XML documents used in the SMC Web Service use numeric identifiers for various resources or entities. Common numerical IDs used are:

Name	Description	Type
domain-id	The ID of a Domain.	Integer
device-id	The ID of a StealthWatch FlowCollector appliance.	Integer
host-group-id	The ID of a Host Group.	Integer
host-group-ids	The IDs of a Host Group. This is a comma-separated list of Host Group Ids	String
spi	The ID of a service as defined by the Service Definitions.	Integer
application-id	The ID of an application as defined by the Application Definitions.	Integer

If the user of the SMC Web Service would like to convert these IDs into string names of the resources, then the user must:

1. Launch the SMC Graphical User Interface (GUI) through Java Web Start.
2. Select the Domain of interest from the tree on the left.
3. Right-click and select "Properties".
4. Select the tab named "Export".
5. Make sure the option "Export All configuration" is selected.
6. Click "Export" and select a file location.
7. Open the exported XML file in your favorite text editor.

The exported XML file will contain the current configuration of the Domain and may serve as a lookup for the IDs listed above.

2.8 Building Web Service Requests from the SMC GUI

It is possible to extract the XML required for a Web Service call from the SMC GUI. This way you may use the SMC GUI to build and fine-tune a query and then cut-and-paste the generated XML into the code or script that is making the Web Service call.

In order to achieve this, the Java Web Start Console must be visible while the SMC GUI is running:

On Windows:

1. From the “Start” menu, select “Control Panel”.
2. Double-click the “Java” item to open the Java control panel.
3. On the “Advanced” tab, make sure that “Java console” -> “Show console” is enabled.



On Mac OS X:

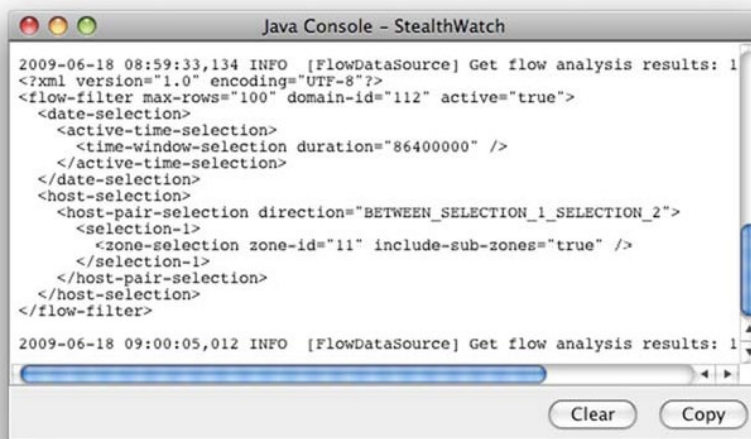
1. Open the folder “Applications” -> “Utilities” -> “Java”
2. Launch the “Java Preferences” application
3. On the “Advanced” tab, make sure that “Java console” -> “Show console” is enabled.



When you next launch the SMC GUI using Java Web Start, a console window will appear that will show logging information. Part of this information will be the XML for any queries that the SMC GUI is making to

SMC Web Services Programming Guide

the SMC Server. You can cut-and-paste this XML into the code or script that will make the Web Service call.



```
2009-06-18 08:59:33,134 INFO [FlowDataSource] Get flow analysis results: 1
<?xml version="1.0" encoding="UTF-8"?>
<flow-filter max-rows="100" domain-id="112" active="true">
  <date-selection>
    <active-time-selection>
      <time-window-selection duration="86400000" />
    </active-time-selection>
  </date-selection>
  <host-selection>
    <host-pair-selection direction="BETWEEN_SELECTION_1_SELECTION_2">
      <selection-1>
        <zone-selection zone-id="11" include-sub-zones="true" />
      </selection-1>
    </host-pair-selection>
  </host-selection>
</flow-filter>

2009-06-18 09:00:05,012 INFO [FlowDataSource] Get flow analysis results: 1
```

Clear Copy

3 Reference

3.1 getDSCPTraffic

3.1.1 Request

The request takes the form of a `dscp-traffic-filter` XML element

```
<dscp-traffic-filter domain-id="104" />
    <date-selection>
        :
    </date-selection>
    <device-selection>
        <interface-selection
            device-id="602" exporter-
            ip="10.10.10.10"
            interface-id="2" />
    </device-selection>
</dscp-traffic-filter>
```

The `dscp-traffic-filter` element has the following attributes:

Name	Description	Type	Use
domain-id	ID of the Domain to be queried.	Integer	Required

The following sections describe the sub-elements of the `dscp-traffic-filter`. These sub-elements must appear in the order described above. The `<date-selection>` sub-element is optional, but the `<device-selection>` sub-element is required.

3.1.1.1 Date and Time Filtering

The request may, optionally, filter the returned records based on date and time:

```
<date-selection>
    :
</date-selection >
```

The `date-selection` element may contain any of the following sub-elements:

```
time-range-selection
time-window-selection
day-selection
```

See 4.1 for more information.

NOTE: If the `<date-selection>` xml is missing, the date/time filter will default to the last 12 hours.

3.1.1.2 Device Filtering

The request will filter the returned records based on the exporter/interface selection. This is a required element:

```
<device-selection>
```

```
<interface-selection . . . />
</device-selection >
```

The `device-selection` element must contain the sub-element:

- `interface-selection`
See 4.2.3 for more information.

3.1.2 Response

The response takes the form of a `dscp-traffic-list` element that contains zero or more `dscp-traffic` elements:

```
<dscp-traffic-list>
  <dscp-traffic
    domain-id="116"
    device-id="130"
    retention="300"
    exporter-ip="10.10.10.10"
    if-index="2"
    time="2012-07-12T12:30:00Z"
    dscp="10"
    traffic-in"46296"
    traffic-out"47214" />
</dscp-traffic-list>
```

The `dscp-traffic` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the traffic was reported.	Integer	Optional
device-id	The ID of the StealthWatch FlowCollector which reported this traffic.	Integer	Optional
retention	The time duration (in seconds) of the reported traffic.	Integer	Optional
exporter-ip	The exporter that observed this traffic.	Integer	Optional
if-index	The interface of the exporter that observed this traffic.	Integer	Optional
time	The end time that the traffic was observed.	ISO8601 Date	Optional
dscp	The DSCP(differentiated services code point) value associated with this traffic.	Integer	Optional
traffic-in	Traffic reported as bps that is received by an interface on a DiffServ-aware router in the monitored network.	Long	Optional
traffic-out	Traffic reported as bps that is sent by the interface on a DiffServ-aware router in the monitored network.	Long	Optional

3.2 getFlows

3.2.1 Request

The request takes the form of a `flow-filter` XML element:

```
<flow-filter max-rows="100"
            domain-id="104"
            remove-duplicates="true"
            order-by="TOTAL_PACKETS"
            order-by-desc="true" />

    <date-selection>
        :
    </date-selection>

    <device-selection>
        :
    </device-selection>

    <host-selection>
        :
    </host-selection>

    <services>. . .</services>

    <ports>. . .</ports>

    <protocols>. . .</protocols>

    <applications>. . .</applications>

    <traffic>
        :
    </traffic>

    <network-performance>
        :
    </network-performance>

    <as-numbers>. . .</as-numbers>

    <dscps>. . .</dscps>

    <vlan-ids>. . .</vlan-ids>

    <mpls-labels>. . .</mpls-labels>

    <client-ports>. . .</client-ports>

    <query>
        :
    </query>

    <flow-action>denied</flow-action>

</flow-filter>
```

The `flow-filter` element has the following attributes:

Name	Description	Type	Use
<code>domain-id</code>	ID of the Domain to be queried.	Integer	Required
<code>max-rows</code>	The maximum number of rows to be returned in the response.	Integer	Optional Default of 2000
<code>remove-duplicates</code>	De-duplicate flows capability	Boolean	Optional Default of false
<code>order-by</code>	Valid values are: <i>TOTAL_BYTES,</i> <i>TOTAL_PACKETS,</i> <i>TOTAL_BYTE_RATE,</i> <i>TOTAL_PACKET_RATE,</i> <i>CLIENT_BYTES,</i> <i>CLIENT_PACKETS,</i> <i>CLIENT_BYTE_RATE,</i> <i>CLIENT_PACKET_RATE,</i> <i>SERVER_BYTES,</i> <i>SERVER_PACKETS,</i> <i>SERVER_BYTE_RATE,</i> <i>SERVER_PACKET_RATE,</i> <i>RTT_MINIMUM,</i> <i>RTT_AVERAGE,</i> <i>RTT_MAXIMUM,</i> <i>SRT_MINIMUM,</i> <i>SRT_AVERAGE,</i> <i>SRT_MAXIMUM,</i> <i>CONNECTIONS,</i> <i>RETRANSMITS</i>	String	Optional
<code>order-by-desc</code>	This specified whether order-by value is processed in descending(true) or ascending(false) order	Boolean	Required if order-by exists
<code>include-interface-data</code>	Allows you to determine whether or not interface data is included in your flow query.	Boolean	Optional Default of true

The following sections describe the sub-elements of the `flow-filter`. These sub-elements are optional and must appear in the order described above.

3.2.1.1 Date and Time Filtering

NOTE: If the `<date-selection>` xml is missing, the date/time filter will default to the last 5 minutes.

The request may, optionally, filter the returned records based on date and time:

```
<date-selection>
```

```
      :  
</date-selection >
```

The `date-selection` element must contain one of the following sub-elements:

- `time-range-selection`
See 4.1.1 for more information.
- `time-window-selection`
See 4.1.2 for more information.
- `day-selection`
See 4.1.3 for more information.

3.2.1.2 Device Filtering

The request may, optionally, filter the returned records based on the associated device or devices:

```
<device-selection>  
      :  
</device-selection >
```

The `device-selection` element must contain one of the following sub-elements:

- `device-list-selection`
See 4.2.1 for more information.
- `exporter-selection`
See 4.2.2 for more information.
- `interface-selection`
See 4.2.3 for more information.

3.2.1.3 Host Filtering

The request may, optionally, filter the returned records based on the associated host or hosts, Host Groups, VM servers, VMs, IP Address Ranges:

```
<host-selection>  
      :  
</host-selection>
```

The `host-selection` element must contain the following sub-element:

- `host-pair-selection`
See 4.3.6 for more information.

3.2.1.4 Services Filtering

The request may, optionally, filter the returned records based on the user-defined services:

```
<services exclude="false">1,2,3,4,26</services>
```

The `services` element contains a comma separated list of SPIs (service profile ids). By looking at the exported configuration, you can determine the SPI. Find the `services-definitions` element, then find the `service name` attribute of the `services` element that you are looking for. The associated `profile` attribute will contain the SPI needed for this filter.

The `services` element supports the following attribute:

Name	Description	Type	Use
exclude	Specify whether to include (=false) or exclude (=true) the flows with the services specified	Boolean	Optional Default is 'false'

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified services. If the exclude attribute is 'true', then a flow is considered to match this constraint if it the flow does NOT match any of the services specified.

NOTE: If flow does not match to any user defined services, the SPI assigned to flow will be raw protocol number plus the constant '60000'. In order to filter by ICMP type, then the SPI will be the ICMP type plus the constant 60256.

Examples:

Filter by Protocol 3pc (protocol number = 34)

```
<services>60034</services>
```

Filter by ICMP type Echo Reply (ICMP Type = 0):

```
<services>60256</services>
```

3.2.1.5 Ports Filtering

The request may, optionally, filter the returned records based on the UDP/TCP port:

```
<ports exclude="true">53/tcp,53/udp</ports>
```

The `ports` element contains a comma separated list of port/protocol values. The value for the protocol portion is either TCP or UDP. The value for the port is the actual port number.

The `ports` element supports the following attribute:

Name	Description	Type	Use
exclude	Specify whether to include (=false) or exclude (=true) the flows with the ports/protocols specified.	Boolean	Optional Default is 'false'

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified ports/protocols. If the exclude attribute is 'true', then a flow is considered to match this constraint if it the flow does NOT match any of the ports/protocols.

3.2.1.6 Protocols Filtering

The request may, optionally, filter the returned records based on the IP protocol:

```
<protocols exclude="true">6,34,114</protocols>
```

The `protocols` element contains a comma-separated list of protocol numbers. The values for the protocol numbers are the actual raw value.

The `protocols` element supports the following attribute:

Name	Description	Type	Use
exclude	Specify whether to include (=false) or exclude (=true) the flows with the protocols specified.	Boolean	Optional Default is 'false'

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified protocols. If the exclude attribute is 'true', then a flow is considered to match this constraint if it the flow does NOT match any of the protocols specified.

3.2.1.7 Applications Filtering

The request may, optionally, filter the returned records based on the user-defined applications:

```
<applications exclude="false">129,165,124</applications>
```

The `applications` element contains a comma separated list of Application IDs. By looking at the exported config, you can determine the application id. Find the `application-list` element, and then find the `name` attribute of the `application` element that you are looking for. The associated `id` attribute will contain the application id needed for this filter.

The `applications` element supports the following attribute:

Name	Description	Type	Use
exclude	Specify whether to include (=false) or exclude (=true) the flows with the applications specified	Boolean	Optional Default is 'false'

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified applications. If the exclude attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the applications specified.

3.2.1.8 Traffic Statistics Filtering

The request may, optionally, filter the returned records based on traffic statistics:

```
<traffic>
  <client>
    <bytes-range low-value="100" high-value="20000" />
    <packets-range low-value="100" high-value="20000" />
  </client>
  <server>
    <bytes-range high-value="20000" />
    <packets-range low-value="100" high-value="20000" />
  </server>
  <total>
    <bytes-range low-value="100" />
    <packets-range low-value="100" high-value="20000" />
  </total>
</traffic>
```

The `traffic` element contains constraints on the byte and packets count on the flow for the client, server or total. Each constraint must contain one or more of the following attributes:

Name	Description	Type	Use
low-value	Lower bound for the constraint.	Integer	Optional
high-value	Upper bound for the constraint.	Integer	Optional

The attributes are interpreted as follows:

- If the `low-value` is not present, then the constraint is interpreted as LESS THAN the `high-value`.
- If the `high-value` is not present, then the constraint is interpreted as GREATER THAN the `low-value`.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

3.2.1.9 Network Performance Statistics Filtering

The request may, optionally, filter the returned records based on network performance statistics:

```
<network-performance>
  <total-connections low-value="1" high-value="2" />
  <total-retransmissions low-value="1" high-value="2" />
  <round-trip-time>
    <min low-value="1" high-value="2" />
    <avg low-value="1" high-value="2" />
    <max low-value="1" high-value="2" />
  </round-trip-time>
  <server-response-time>
    <min low-value="1" high-value="2" />
    <avg low-value="1" high-value="2" />
    <max low-value="1" high-value="2" />
  </server-response-time>
</network-performance>
```

The `network performance` element contains constraints on the performance statistics maintained for each flow. Each constraint must contain one or more of the following attributes:

Name	Description	Type	Use
low-value	Lower bound for the constraint.	Integer	Optional
high-value	Upper bound for the constraint.	Integer	Optional

The attributes are interpreted as follows:

- If the `low-value` is not present, then the constraint is interpreted as LESS THAN the `high-value`.
- If the `high-value` is not present, then the constraint is interpreted as GREATER THAN the `low-value`.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

NOTE: The unit for the time values is milliseconds.

3.2.1.10 Autonomous System Number (ASN) Filtering

The request may, optionally, filter the returned records based on ASN:

```
<as-numbers exclude="true">11</as-numbers>
```

The `as-numbers` element simply contains a comma-separated list of the ASNs of interest.

The `as-numbers` element supports the following attribute:

Name	Description	Type	Use
exclude	Specify whether to include (=false) or exclude (=true) the as-numbers.	Boolean	Optional Default is 'false'

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified as-numbers. If the exclude attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the as-numbers specified.

NOTE: This constraint should only be used if the device selected in the `device-selection` is a StealthWatch FlowCollector for NetFlow appliance. Otherwise an error will be returned.

3.2.1.11 Differentiated Services Code Point (DSCP) Filtering

The request may, optionally, filter the returned records based on DSCP:

```
<dscps>28,18,12</dscps>
```

The `dscps` element simply contains a comma-separated list of the DSCPs of interest.

The `dscps` element supports the following attribute:

Name	Description	Type	Use
exclude	Specify whether to include (=false) or exclude (=true) the dscps.	Boolean	Optional Default is 'false'

NOTE: If the exclude attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified DSCPs. If the exclude attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the DSCPs specified.

3.2.1.12 Virtual LAN IDs Filtering

The request may, optionally, filter the returned records based on Virtual LAN IDs:

```
<vlan-ids>1,2,3</vlan-ids>
```

The `vlan-ids` element simply contains a comma-separated list of the Virtual LAN IDs of interest.

The `vlan-ids` element supports the following attribute:

Name	Description	Type	Use
<code>exclude</code>	Specify whether to include (=false) or exclude (=true) the VLAN IDs.	Boolean	Optional Default is 'false'

NOTE: If the `exclude` attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified VLAN IDs. If the `exclude` attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the VLAN IDs specified.

3.2.1.13 MPLS Labels Filtering

The request may, optionally, filter the returned records based on MPLS labels

```
<mpls-labels>9321,45782</mpls-labels>
```

The `mpls-labels` element simply contains a comma-separated list of the Virtual LAN IDs of interest.

The `mpls-labels` element supports the following attribute:

Name	Description	Type	Use
<code>exclude</code>	Specify whether to include (=false) or exclude (=true) the MPLS labels.	Boolean	Optional Default is 'false'

NOTE: If the `exclude` attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified `MPLS labels`. If the `exclude` attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the `MPLS labels` specified.

3.2.1.14 Client Ports Filtering

The request may, optionally, filter the returned records based on MPLS labels:

```
<client-ports>53921,65421</client-ports>
```

The `client-ports` element simply contains a comma-separated list of the client ports of interest.

The `client-ports` element supports the following attribute:

Name	Description	Type	Use
<code>exclude</code>	Specify whether to include (=false) or exclude (=true) the client ports.	Boolean	Optional Default is 'false'

NOTE: If the `exclude` attribute is 'false', then a flow is considered to match this constraint if it matches AT LEAST ONE of the specified client ports. If the `exclude` attribute is 'true', then a flow is considered to match this constraint if the flow does NOT match any of the client ports specified.

3.2.1.15 Payload Filtering

The request may, optionally, filter the returned records based contents of the payload:

```
<query>
  <payload-match-all>get</payload-match-all>
  <payload-match-any>ssh</payload-match-any>
  <payload-not-match-all>dns</payload-not-match-all>
</query>
```

The `query` element supports 3 sub-elements for matching text in payloads as seen above in the sample, and are described below.

Name	Description	Type	Use
payload-match-all	This element will appear for each string in match request. All strings must be found for this flow to be selected	String	Optional
payload-match-any	This element will appear for each string in match request. If any one of the strings are found, this flow will be selected	String	Optional
payload-not-match-all	This element will appear for each string in match request. All strings must match in order for the flow to be ignored	String	Optional

NOTE: Both client and server payloads are examined in the query.

3.2.1.16 Flow Action

The request may, optionally, filter the returned records based on the Cisco ASA `flow-action` of `permitted` or `denied`:

```
<flow-action>permitted</flow-action>
```

The `flow-action` element simply contains one of 2 values: `permitted` or `denied`.

3.2.2 Response

The response takes the form of a `flow-list` element that contains zero or more `flow` elements:

```
<flow-list>
  <flow>
    <client>
      :
    </client>
    <server>
      :
    </server>
    <application>..</application>
    <rtt. . ./>
    <src. . ./>
  </flow>
</flow-list>
```

The `flow` element contains the following attributes:

Name	Description	Type	Use
id	A unique number that identifies the flow.	Long	Required
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
start-time	The time at which this flow began.	ISO8601 Date	Required
last-time	The time at which this flow was last observed to be active.	ISO8601 Date	Required
active-duration	The number of seconds the flow has been active.	Integer	Optional
protocol	The protocol number	Integer	Required
service-id	The id of the service that this flow is using as defined by the Service Definitions for the Domain.	Integer	Required
application-id	The application that this flow is using as defined by the Application Definitions for the Domain.	Integer	Required
service	The UDP or TCP port number that defines the service used by this flow.	Integer	Required
connections	The number of TCP connections that occur during a flow.	Integer	Optional
retransmits	The number of TCP packets that were retransmitted during the flow.	Integer	Optional
vlan-id	The number identifying a virtual LAN associated with the flow.	Integer	Optional
mpls-label	The Multi-Protocol Label Switching label associated with the flow.	Integer	Optional
total-bytes	The total payload bytes transmitted by both client and server.	Long	Optional

The `client` and `server` sub-elements will both exist and can look like this:

```

<client> or <server>
  <flags. . ./>
  <payload. . ./>
  <interface-list>
    <interface. . ./>
    :
  </interface-list>
</client> or </server>

```

The `client` and `server` sub-elements contain the following attributes:

Name	Description	Type	Use
ip-address	The IP address of the host.	String	Required
xlate-ip-address	The translated IP address (i.e., as altered by a network address translation device) of the host	String	Optional
host-name	The name of the host.	String	Optional
country	The country that the host belongs to.	String	Optional
host-group-ids	The comma separated list of Host Group IDs of the Host Groups that the host belongs to.	String	Required
vserver-id	The VM server id on which this host exists.	Integer	Optional
vserver-ip-address	The VM server ip-address on which this host exists.	String	Optional
vserver-name	The VM server name on which this host exists.	String	Optional
vmachine-id	The virtual machine id associated with the host.	Integer	Optional
vmachine-name	The virtual machine name associated with the host.	String	Optional
mac-address	The MAC address observed for this host.	string	Optional
port	The last TCP or UDP port number used by the host to receive packets.	Integer	Required
xlate-port	The port used by the translated host.	Integer	Required
bytes	The number of bytes sent by the host.	Long	Required
packets	The number of packets sent by the host.	Packets	Required
asn	The ASN associated with the client/server. NOTE: this attribute will only have a meaningful value if a StealthWatch FlowCollector for NetFlow observed the flow.	Long	Optional

There are 3 sub-elements that may be included in the `client` and the `server` sub-elements, the `flags` sub-element, the `interface-list` sub-element and the `payload` sub-element. These will be described in the sections below.

3.2.2.1 Flags

Each of the `client` and `server` elements also contains a `flags` sub-element that contains the following attributes:

Name	Description	Type	Use
syn	The number of TCP packets sent by the host with the SYN header flag set.	Integer	Optional

syn-ack	The number of TCP packets sent by the host with the SYN and ACK header flags set.	Integer	Optional
rst	The number of TCP packets sent by the host with the RST header flag set.	Integer	Optional
fin	The number of TCP packets sent by the host with the FIN header flag set.	Integer	Optional

3.2.2.2 Exporters

Both the `client` and `server` elements may contain an `interface-list` element that describes the interfaces that have seen this flow in the given direction:

```
<flow
w    id="120448"
    domain-id="117"
    device-id="118"
    start-time="2011-04-07T11:48:30Z"
    last-time="2011-04-07T11:48:30Z"
    active-duration="0"
    protocol="17"
    service-id="64"
    application-id="170"
    service="1027">
  <client
    ip-address="11.11.166.53" host-group-ids="61627"
    country="US" port="63081" bytes="4314800"
    packets="700" asn="46554">
    <flags syn="0" syn-ack="0" rst="0" fin="0" />
    <interface-list>
      <interface
        exporter-ip="10.10.10.10"
        if-index="1"
        direction="OUTBOUND"
        bytes="1401408"
        packets="216" />
      <interface
        exporter-ip="10.10.10.10"
        if-index="2"
        direction="OUTBOUND"
        bytes="4314800"
        packets="700" />
    </interface-list>
  </client>
  <server
    ip-address="12.12.173.120" host-group-ids="61627"
    country="US" port="1027" bytes="1401408"
    packets="216" asn="47440">
    <flags syn="0" syn-ack="0" rst="0" fin="0" />
    <interface-list>
      <interface
        exporter-ip="10.10.10.10"
        if-index="1"
        direction="INBOUND"
        bytes="4314800"
        packets="700"
        dscp="0" />
    </interface-list>
  </server>
</flow>
```

```

        <interface
            exporter-ip="10.10.10.10"
            if-index="2" direction="INBOUND"
            bytes="1401408" packets="216" dscp="0" />
        </interface-list>
    </server>
</flow>

```

The `interface` element contains the following attributes:

Name	Description	Type	Use
exporter-ip	The IP address of the NetFlow or sFlow exporter that observed this flow.	String	Required
if-index	The index number of the interface that this flow traversed.	Integer	Required
dscp	The DSCP associated with the client/server. NOTE: this attribute will only have a meaningful value if a StealthWatch FlowCollector for NetfFow observed the flow.	Integer	Optional
direction	The direction is one of 2 values: INBOUND for data received by the interface, or OUTBOUND for data sent by the interface.	String	Optional
bytes	The total number of bytes sent by this interface	Long	Optional
packets	The total number of packets sent by this interface	Long	Optional
min-ttl	The smallest number of host/links over which the first packet from this host may be routed.	Integer	Optional
max-ttl	The largest number of host/links over which the first packet from this host may be routed.	Integer	Optional
flow-action	If the exporter type is Cisco ASA then this value will be present and values will be either 'permitted' or 'denied'	String	Optional

3.2.2.3 Packet Data

There may be additional data in the flow describing actual packet data sampled from the flow:

```

<flo
w    id="80049"
      domain-id="117"
      device-id="118"
      start-time="2011-04-07T08:10:34Z"
      last-time="2011-04-07T08:15:16Z"
      active-duration="282000"
      protocol="6"
      service-id="3"
      application-id="39"
      service="80"
      connections="1"
      retransmits="0">

```



```

<client
  ip-address="10.201.3.25"
  host-group-ids="155,1545"
  country="XR"
  port="58014"
  bytes="1174"
  packets="7">
  <flags syn="0" syn-ack="0" rst="0" fin="0" />
  <payload>
    <![CDATA[ POST /hc/request.rep HTTP/]]>
  </payload>
</client>
<server
  ip-address="208.89.13.133"
  host-group-ids="61627"
  host-name="server.iad.liveperson.net"
  country="US"
  port="80"
  bytes="0"
  packets="0">
  <flags syn="0" syn-ack="0" rst="0" fin="0" />
  <payload>
    <![CDATA[ HTTP/1.1 200 OK..Date: Thu]]>
  </payload>
</server>
<application flowsensor="23" />
<rtt min="19" avg="19" max="19" />
<srt min="2" avg="2" max="2" />
</flow>

```

Both the `client` and `server` elements contain a `payload` element that contains the first 26 bytes from the first packet observed from that host. The data is provided in ASCII format.

3.2.2.4 Application Data

The `application` element is a sub-element of the `flow` element and can contain the following attributes:

Name	Description	Type	Use
<code>flowsensor</code>	The id of the application that was discovered by the Flowsensor application discovery process.	Integer	Optional
<code>nbar</code>	The id of the application that was discovered by examining the CISCO netflow data.	Integer	Optional
<code>packetshaper</code>	The id of the application that was discovered by examining the data sent by the PacketShaper Appliance.	Integer	Optional

NOTE: The ID's returned above are explicit to the source of the application discovery.

3.2.2.5 Performance Statistics

The `rtt` and `srt` elements are both sub-elements of the `flow` element. Each of these elements can contain the following attributes:

Name	Description	Type	Use
Min	The average of the least amounts of time in milliseconds.	Integer	Optional
Max	The average of the greatest amounts of time in milliseconds	Integer	Optional
Avg	The average amount of time in milliseconds	Integer	Optional

3.3 getSecurityEvents

NOTE: 'getCiEvents' is deprecated and has been replaced with 'getSecurityEvents' in version v6.5. The 'getCiEvents' service will not be supported in future releases.

3.3.1 Request

The request takes the form of a `security-event-filter` XML element:

```
<security-event-filter max-rows="2000" domain-id="104">
  <date-selection>
    :
  </date-selection>
  <device-selection>
    :
  </device-selection>
  <host-selection>
    :
  </host-selection>
  <types> .. </types>
  <ports> .. </ports>
  <hit-count .. />
  <ci-points .. />
</security-event-filter>
```

The `security-event-filter` element has the following attributes:

Name	Description	Type	Use
domain-id	ID of the Domain to be queried.	Integer	Required
max-rows	The maximum number of rows to be returned in the response.	Integer	Optional Default of 2000

The following sections describe the sub-elements of the `security-event-filter`. These sub-elements are optional and must appear in the order described above.

3.3.1.1 Date and Time Filtering

The request may, optionally, filter the returned records based on time:

```
<date-selection>
```

```
      :  
</date-selection >
```

The `date-selection` element must contain one of the following sub-elements:

- `active-time-selection`
See 4.1.5 for more information.
- `first-last-time-selection`
See 4.1.6 for more information.

3.3.1.2 Device Filtering

The request may, optionally, filter the returned records based on the associated device or devices:

```
<device-selection>  
      :  
</device-selection >
```

- `device-list-selection`
See 4.2.1 for more information.

3.3.1.3 Host Filtering

The request may, optionally, filter the returned records based on associated the host or hosts:

```
<host-selection>  
      :  
</host-selection >
```

The `host-selection` element can contain the `host-pair-selection`. See 4.3.6 for more information.

3.3.1.4 Security Event Type Filtering

The request may, optionally, filter the returned records based on Security Event type:

```
<types>50,49,2,20,23,44</types>
```

The `types` element is simply a comma separated list of Security Event Type IDs. See 4.6 for the list of Security Events and the corresponding IDs.

3.3.1.5 Port Filtering

The request may, optionally, filter the returned records based on TCP or UDP port number:

```
<ports>33-55/udp,77/tcp</ports>
```

The `ports` element contains a comma separated list of port/protocol values. The value for the protocol portion is either TCP or UDP. The value for the port is the actual port number.

3.3.1.6 Hit Count Filtering

The request may, optionally, filter the returned records based on the number of hits that occurred.

```
<hit-count low-value="10" high-value="200" />
```

The `hit-count` sub-element contains the following attributes:

Name	Description	Type	Use
<code>low-value</code>	Lower bound for the constraint.	Integer	Optional
<code>high-value</code>	Upper bound for the constraint.	Integer	Optional

The attributes are interpreted as follows:

- If the `low-value` is not present, then the constraint is interpreted as LESS THAN the `high-value`.
- If the `high-value` is not present, then the constraint is interpreted as GREATER THAN the `low-value`.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

3.3.1.7 Concern Index Filtering

The request may, optionally, filter the returned records based on the value of the value of the Concern Index.

```
<ci-points low-value="3" high-value="4" />
```

The `ci-points` sub-element contains the following attributes:

Name	Description	Type	Use
<code>low-value</code>	Lower bound for the constraint.	Integer	Optional
<code>high-value</code>	Upper bound for the constraint.	Integer	Optional

The attributes are interpreted as follows:

- If the `low-value` is not present, then the constraint is interpreted as LESS THAN the `high-value`.
- If the `high-value` is not present, then the constraint is interpreted as GREATER THAN the `low-value`.
- If both attributes are preset, then the constraint is interpreted as BETWEEN the two values.

3.3.2 Response

The response takes the form of a `security-event-list` element that contains zero or more `security-event` elements:

```
<security-event-list>
  <security-event
    domain-id="117"
    device-id="118"
    start-time="2011-04-07T04:01:56Z"
    last-time="2011-04-07T16:43:56Z"
    ci-points="492984"
    total-hits="988">
    <source
      ip-address="128.9.160.132"
      host-group-ids="61627"
      host-name="jar.isi.edu"
      country="US" />
  </security-event>
</security-event-list>
```

SMC Web Services Programming Guide

```

    <target
      ip-address="209.182.184.0"
      host-group-ids="1519"
      country="US" />
    <details-list>
      <details type="21" hit-count="984" ci-points="49984" />
      <details type="1" hit-count="4" ci-points="0" />
    </details-list>
  </security-event>
<security-event>
  :
</security-event>
:
</security-event-list>

```

The `security-event` element contains the following attributes:

Name	Description	Type	Use
Id	Unique ID assigned to the Security Event: NOT IN real output	Integer	Optional
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
start-time	The time at which this Security Event began.	ISO8601 Date	Required
last-time	The time at which this Security Event was last observed to be active.	ISO8601 Date	Required
ci-points	The total number of Concern Index points that were generated by the Security Event.	Integer	Required
total-hits	The total number of hits generated during the Security Event.	Integer	Required

The `source` and `target` sub-elements contain the following attributes:

Name	Description	Type	Use
ip-address	The IP address of the host.	String	Required
host-name	The name of the host.	String	Optional
country	The country that the host belongs to.	String	Required
host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required

The `details-list` element contains one or more `details` elements that break down the Security Event by type. Each `details` element contains the following attributes:

Name	Description	Type	Use
type	The ID of the Security Event type. See 4.6 for more information.	Integer	Required

hit-count	The number of hits for this particular Security Event type.	Integer	Required
ci-points	The Concern Index points for this particular Security Event type.	Integer	Required

3.4 getHostSnapshot

3.4.1 Request

The request takes the form of a `host-filter` XML element:

```
<host-filter domain-id="104">
  <date-selection>
    :
  </date-selection>
  <device-selection>
    :
  </device-selection>
  <host-selection>
    :
  </host-selection>
</host-filter>
```

The `host-filter` element has the following attributes:

Name	Description	Type	Use
domain-id	ID of the Domain to be queried.	Integer	Required

The following sections describe the sub-elements of the `host-filter`. These sub-elements are optional and must appear in the order described above.

3.4.1.1 Date and Time Filtering

The request may, optionally, filter the returned records based on time:

```
<date-selection>
  :
</date-selection >
```

The `date-selection` element must contain one of the following sub-elements:

- `day-selection`
See 4.1.3 for more information.

3.4.1.2 Device Filtering

The request may, optionally, filter the returned records based on the associated device or devices:

```
<device-selection>
  :
</device-selection >
```

The `device-selection` element must contain one of the following sub-elements:

- `device-list-selection`
See 4.2.1 for more information.

3.4.1.3 Host Filtering

The request must specify the host of interest:

```
<host-selection>
  <ip-address-selection value="10.202.4.131"/>
</host-selection >
```

The `host-selection` element must contain one of the following sub-elements:

- `ip-address-selection`
See 4.3.4 for more information.

3.4.2 Response

The response takes the form of a `host-snapshot` element:

```
<host-snapshot
  domain-id="117"
  ip-address="10.202.15.73"
  host-group-ids="154,1545"
  host-name="vcenter.lancope.local"
  country="XR"
  time="2011-04-07T17:47:40Z">
  <status-list>
    :
  </status-list>
  <host-information-list>
    :
  </host-information-list>
  <security-list>
    :
  </security-list>
  <touched-list>
    :
  </touched-list>
  <traffic-list>
    :
  </traffic-list>
  <ci-events>
    :
  </ci-events>
  <flows>
    :
  </flows>
  <exporters>
    :
  </exporters>
  <alarm-counts-list>
    :
  </alarm-counts-list>
  <alarm-list>
    :
  </alarm-list>
  <identity-session-list>
    :
```

```

</identity-session-list>
<user-activity-list>
  :
</user-activity-list>
<dhcp-lease-list>
  :
</dhcp-lease-list>
<host-note-list>
  :
</host-notes-list>
</host-snapshot>

```

The `host-snapshot` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
ip-address	The IP address of the host.	String	Required
host-name	The name of the host.	String	Optional
country	The country that the host belongs to.	String	Required
host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required
time	The timestamp of when the request was made	ISO8601 Date	

The optional sub-elements contain various information regarding the behavior of the host during the time specified in the filter and will be described in the subsequent sections.

3.4.2.1 Status

The response may contain a `status-list` element:

```

<status-list>
  <status
    domain-id="104"
    device-id="117"
    value="active"
    first-seen="2010-12-12T20:09:45Z"
    last-seen="2011-02-06T18:21:00Z">
    <mac-address value="00:1e:13:80:d0:c0" vendor="Unknown Vendor"/>
  </status>
  <status ..>
    :
  </status>
  :
</status-list>

```

The `status` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required

value	The current status of the host.	Enumeration of "active", "inactive" or "phantom"	Required
first-seen	The time at which this host was first observed.	ISO8601 Date	Required
last-seen	The time at which this host was last observed.	ISO8601 Date	Required

Optionally, there could be `mac-address` sub-element that contains the following attributes:

Name	Description	Type	Use
value	The MAC address observed for this host.	String	Optional
vendor	The name of the vendor that is assigned this MAC address.	String	Optional

3.4.2.2 Host Information

The response may contain a `host-information-list` element:

```

<host-information-list>
  <host-information
    domain-id="117"
    device-id="118"
    ip-address="10.202.15.73" host-
    group-ids="154,1545" host-
    name="vcenter.lancope.local"
    country="XR">
    <service-profile-status>
      <server>1:S60256,S60264,S3,O12489/tcp</server>
      <client>1:S4,S1,S29,S48,S23,S36,S14,S34,S3</client>
    </service-profile-status>
    <application-activity>
      <server>,186,170,169,168,</server>
      <client>,51,186,171,187,184,185,190,188,58,</client>
    </application-activity>
    <os>1897979539</os>
  </host-information>
  <host-information ..>
    :
  </host-information>
  :
</host-information-list>

```

The `host-information` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
ip-address	The IP address of the host.	String	Required
host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required

country	The country that the host belongs to.	String	Required
service-profile-status	The services that have been observed for this host as either a Server or Client. See 4.4 for details of the format	String	Optional
application-activity	The applications that have been observed for this host as either a Server or Client.	String	Optional
os	The operating system code	String	Optional

3.4.2.3 Security

The response may contain a `security-list` element:

```
<security-list>
  <security domain-id="104" device-id="117"
    <concern-index value="8875685" threshold="1000000"/>
    <target-index value="15910" threshold="50000"/ >
    <file-sharing-index value="91161000" threshold="500000"/>
  </security>
  <security ..>
    :
  </security>
  :
</security-list>
```

The `security` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required

Each sub-element of the `security` element describes the status of the Concern Index, Target Index and File Sharing Index for the host and contains the following attributes:

Name	Description	Type	Use
value	The current value of the index.	Integer	Required
threshold	The alarm threshold that is currently in effect for the index.	Integer	Required

3.4.2.4 Touched

The response may contain a `touched-list` element:

```
<touched-list>
  <touched
    domain-id="115"
    device-id="252"
    been-touched="false"
    has-touched="true"/>
</touched>
```

```

        <touched ..>
          :
        </touched>
      :
    </touched-list>

```

The `touched` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
been-touched	Indicates if this host has communicated with a host with High Concern Index.	Boolean	Required
has-touched	Indicates if this host has a High Concern Index value and has communicated with other hosts.	Boolean	Required

3.4.2.5 Traffic

The response may contain a `traffic-list` element:

```

<traffic-list>
  <traffic domain-id="117" device-id="118">
    <five-min threshold="100000000" udp-percent="2">
      <in max-bps="119976" />
      <out max-bps="8424" />
    </five-min>
    <day threshold="3000000000" data-loss-threshold="0">
      <in
        total-bytes="4656110"
        total-packets="5633"
        total-data-bytes="4431414" />
      <out
        total-bytes="739394"
        total-packets="3682"
        total-data-bytes="593242"
        data-loss="0" />
    </day>
  </traffic>
</traffic-list>

```

The `traffic` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required

The `traffic` element contains 2 sub-elements: `five-min` and `day`.

The `5-min` element contains the following attributes:

Name	Description	Type	Use
threshold	The current value for the 'High Traffic in 5 min' setting	Integer	Required
udp-percent	The percentage of traffic that used the UDP protocol	Integer	Required

The `5-min` element contains 2 sub-elements: `in` and `out`. Each of these contains the following attribute:

Name	Description	Type	Use
max-bps	The highest number of bits per second the host has received(in) or sent(out) for any 5 minute interval over the last 24 hours	Integer	Optional

The `day` element contains the following attributes:

Name	Description	Type	Use
threshold	The current value for the "High Total Traffic in 24 hrs" setting	Integer	Required
data-loss-threshold	The threshold for the Suspect Data Loss alarm, as set on the policy.	Integer	Optional

The `day` element contains 2 sub-elements: `in` and `out`. Each of these contain the following attributes:

Name	Description	Type	Use
Total-bytes	The total number of bytes that the host has sent(out) or received(in), including the IP and TCP header, over the last 24 hours.	Integer	Optional
Total-packets		Integer	Required
Total-data-bytes	The total number of bytes of payload information that the host has sent(out) or received(in) over the last 24 hours.	Integer	Required
Total-loss	The cumulative amount of suspected data loss by the host on the corresponding appliance since the last archive hour.	Integer	Optional 'out' element only

3.4.2.6 CI Events

The response may contain a `ci-events` element:

```
<ci-events>
  <source-high-ci-list>
    <ci-event ..>
      :
```

```

        </ci-event>
        :
    </source-high-ci-list>
    <source-list>
        <ci-event ..>
            :
        </ci-event>
        :
    </source-list>
    <target-list>
        <ci-event ..>
            :
        </ci-event>
        :
    </target-list>
</ci-events>

```

The `ci-events` element may contain 3 sub-elements that contain lists of CI Events in the format described in 3.3.2.

3.4.2.7 Flows

The response may contain a `flows` element:

```

<flows>
  <most-recent>
    <flow connected="10.202.25.46"
      connected-host-group-ids="154,1545"
      start-time="2011-04-07T21:34:16Z"
      last-time="2011-04-07T21:34:16Z"
      protocol="tcp"
      service="https"
      service-id="4"
      bytes-sent="4506"
      bytes-received="2324"
      pkts-sent="20"
      pkts-received="22"
      average-bps="0"
      role="Server"
      total-conn="1"
      total-retrans="1"
      min-rtt="1"
      max-rtt="1"
      avg-rtt="1"
      min-srt="3"
      max-srt="3"
      avg-srt="3"
    </flow>
    :
  </most-recent>
  <highest-traffic>
    <flow ..>
      :
    </flow>
    :
  </highest-traffic>
</flows>

```

The `flow` element contains the following attributes:

SMC Web Services Programming Guide

Name	Description	Type	Use
connected	The IP address of the other host in the flow.	String	Required
connected-host-group-ids	The IDs of the Host Groups that the other host belongs to.	String	Required
connected-vm	The IP address of the host with which the subject host communicated during the flow	String	Optional
start-time	The time at which this flow began.	ISO8601 Date	Required
last-time	The time at which this flow was last observed to be active.	ISO8601 Date	Required
protocol	The IP protocol used in the flow.	String	Required
service	The service used in the flow.	String	Required
service-id	The service used in the flow.	String	Required
bytes-sent	The number of bytes sent by this host.	Integer	Required
bytes-received	The number of bytes received by this host.	Integer	Required
pkts-sent	The number of bytes sent by this host.	Integer	Required
pkts-received	The number of bytes received by this host.	Integer	Required
average-bps	The average rate of traffic (in bits per second) between the hosts in the flow.	Integer	Required
role	The role of this host in the flow.	Enumeration of "Client", "Server" or "Undetermined"	Required
total-conn	The Total TCP Connections from the first SYN to the last ACK that occur during the flow.	Long	Optional
total-retrans	The percentage of TCP packets that were retransmitted during the flow	Long	Optional
min-rtt	The Minimum Round-Trip Time (in milliseconds) required for all the TCP connections to occur in the flow	Long	Optional
max-rtt	The Maximum Round-Trip Time (in milliseconds) required for all the TCP connections to occur in the flow	Long	Optional
avg-rtt	The Average Round-Trip Time (in milliseconds) required for all the TCP connections to occur in the flow	Long	Optional
min-srt	The Minimum Server Response Time (in milliseconds) between the first client request and the first server response among	Long	Optional

	all the TCP connections in the flow		
max-srt	The Maximum Server Response Time between the first client request and the first server response among all the TCP connections in the flow.	Long	Optional
avg-srt	The Average Server Response Time (in milliseconds) between the first client request and the first server response for all the TCP connections in the flow.	Long	Optional

3.4.2.8 Exporters

The response may contain an `exporters` element:

```

<exporters>
  <closest-interface-list>
    <closest-interface
      domain-id="115"
      device-id="252"
      exporter-ip="11.9.102.4"
      if-index="833"
      confidence="100"/>
    <closest-interface ../>
  :
</closest-interface-list>
<active-source-list>
  <interface-status
    domain-id="115"
    device-id="252"
    exporter-ip="11.8.1.101"
    if-index="9">
    <inbound
      current-bps="662"
      maximum-bps="1293"
      average-bps="0"
      current-pps="0"
      maximum-pps="0"
      average-pps="0"
      current-util="0"
      maximum-util="0"/>
    <outbound
      current-bps="662"
      maximum-bps="0"
      average-bps="0"
      current-pps="0"
      maximum-pps="0"
      average-pps="0"
      current-util="0"
      maximum-util="0"/>
    </interface-status>
  <interface-status ../>
  :
</interface-status>
:
</active-source-list>

```

SMC Web Services Programming Guide

```

    <active-dest-list>
      <interface-status ..>
        :
      </interface-status>
      :
    </active-dest-list>
    <today-list>
      <interface-status ..>
        :
      </interface-status>
      :
    </today-list>
  </exporters>

```

The `exporters` element contains the following sub-elements:

- `closest-interface-list`
Determination of which Exporter and Interface is closest to the host.
- `active-source-list`
List of Interfaces that have seen inbound traffic with this host as the source.
- `active-dest-list`
List of interface that have seen outbound traffic with this host as the destination.
- `today-list`
List of interfaces that have seen any traffic to or from this host.

The `closest-interface-list` element contains one or more `closest-interface` elements that each has the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
exporter-ip	The IP address of the exporter that observed this host.	String	Required
if-index	The index number of the Interface that passed traffic for this host.	Integer	Required
confidence	The confidence level, in percent, with the closest interface determination.	Integer	Required

The `active-source-list`, `active-dest-list` and `today-list` all contain one or more `interface-status` elements that each have the flow following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
exporter-ip	The IP address of the exporter that observed this host.	String	Required
if-index	The index number of the Interface that passed traffic for this host.	Integer	Required

In addition, the `interface-status` element contains an `inbound` and `outbound` element that each has the following attributes:

Name	Description	Type	Use
current-bps	The current traffic rate (in bits per second) through the interface.	Integer	Required
maximum-bps	The highest traffic rate (in bits per second) through the interface over the time period requested.	Integer	Required
average-bps	The average traffic rate (in bits per second) through the interface over the time period requested.	Integer	Required
current-pps	The current packet rate (in packets per second) through the interface.	Integer	Required
maximum-pps	The highest packet rate (in packets per second) through the interface over the time period requested.	Integer	Required
average-pps	The average packet rate (in packets per second) through the interface over the time period requested.	Integer	Required
current-util	The current interface utilization (in percent).	Double	Required
maximum-util	The highest interface utilization (in percent) over the time period requested.	Double	Required

3.4.2.9 Alarm Counts

The response may contain an `alarm-counts-list` element:

```
<alarm-counts-list>
  <alarm-counts domain-id="104" device-id="117" source="13" target="0">
    <details alarm-type="7" source="11" target="0"/>
    <details alarm-type="16" source="2" target="0"/>
    :
  </alarm-counts>
  <alarm-counts ..>
    :
  </alarm-counts>
  :
</alarm-counts-list>
```

The `alarm-counts-list` element contains one or more `alarms-counts` elements that have the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required

source	The number of alarms active during the requested time period, where this host was the Source.	Integer	Required
target	The number of alarms active during the requested time period, where this host was the Target.	Integer	Required

Each `details` sub-element of the `alarm-counts` element then breaks down the counts by Alarm Type and has the following attributes:

Name	Description	Type	Use
alarm-type	The ID of the Alarm Type.	Integer	Required
source	The number of alarms active during the requested time period, where this host was the Source.	Integer	Required
target	The number of alarms active during the requested time period, where this host was the Target.	Integer	Required

3.4.2.10 Alarms

The response may contain an `alarm-list` element:

```
<alarm-list>
  <alarm
    domain-id="101"
    device-id="103"
    id="2V-13BN-VMSF-XY9K-K"
    type="35"
    start-time="2011-03-09T23:34:00Z"
    end-time="2011-03-10T00:19:00Z"
    active="false">
    <source ip-address="192.168.1.40"
      host-group-ids="11,28"
      country="US"/>
    <target ip-address="192.168.1.50"
      host-group-ids="11,25"
      country="XR"/>
  </alarm>
  <alarm ..>
    :
  </alarm>
  :
</alarm-list>
```

The `alarm-list` element contains one or more `alarm` elements that have the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
id	The globally unique ID of the alarm.	String	Required

type	The ID of the Alarm type. See 4.5 for more information.	Integer	Required
start-time	The time at which the alarm started.	ISO8601 Date	Required
end-time	The time at which the alarm ended.	ISO8601 Date	Optional
active	Indication if the alarm was active at the time of the request.	Boolean	Required

The `alarm` element contains a `source` and/or `target` sub-element that each has the following attributes:

Name	Description	Type	Use
ip-address	The IP address of the host.	String	Required
host-name	The name of the host.	String	Optional
country	The country that the host belongs to.	String	Required
host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required

3.4.2.11 Identity Session

The response may contain an `identity-session-list` element:

```
<identity-session-list>
  <identity-session
    domain-id="101"
    device-id="170"
    ip-address="192.168.3.100"
    host-group-ids="11,15"
    host-name="some.hostname.local."
    country="XR"
    start-time="2011-03-10T12:31:26Z"
    end-time="2011-03-10T18:06:28Z"
    active="false"
    username="bob"
    vlan="v-1234"
    device-type="phone"
    ad-domain="ms-domain"
    vpn-ip="10.202.1.96">
    <mac-address value="00:ab:cd:ef:12:34" vendor="Acme Inc."/>
    <network-access-device ip-address="192.168.1.10"
      name="ms-activedirectory"
      interface="interface-name" />
    <user-groups identity="group1" security="group2" />
    <server ip-address="10.202.1.1" name="dev" />
  </identity-session>
</identity-session-list>
```

The `identity-session-list` element contains one or more `identity-session` elements that have the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required

SMC Web Services Programming Guide

device-id	The ID of the Cisco ISE appliance that made this observation.	Integer	Required
ip-address	The IP address of the host.	String	Required
host-name	The name of the host.	String	Optional
host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required
country	The country that the host belongs to.	String	Required
start-time	The time at which the session started.	ISO8601 Date	Required
end-time	The time at which the session ended.	ISO8601 Date	Optional
active	Indication if the session was active at the time of the request.	Boolean	Required
username	The username used for this session,	String	Required
vlan	The user's assigned VLAN	String	Optional
device-type	The endpoint's device type as detected by the NAC profiler	String	Optional
ad-domain	The user's Active Directory domain	String	Optional

The `identity-session` element contains four sub-elements that describe the authentication server and Windows domain used for the session.

The `mac-address` element has the following attributes:

Name	Description	Type	Use
value	The MAC address of the host requesting the DHCP lease.	String	Required
vendor	The name of the vendor that has been assigned the MAC address.	String	Optional

The `network-access-device` element has the following attributes:

Name	Description	Type	Use
ip-address	The IP address of the endpoint's network attachment device.	String	Optional
name	The DNS name of the endpoint's network attachment device.	String	Optional
interface	The endpoint's network attachment port.	String	Optional

The `user-groups` element has the following attributes:

Name	Description	Type	Use
identity	The user's provisioned group (OU in LDAP, for instance)	String	Optional
security	The user's TrustSec SGT group	String	Optional

The `server` element has the following attributes:

Name	Description	Type	Use
ip-address	The IP address of the server providing the authentication data.	String	Optional
name	The name given to the server providing the authentication data.	String	Optional

3.4.2.12 User Activity

The response may contain a `user-activity-list` element:

```

<user-activity-list>
  <user-activity
    domain-id="101"
    device-id="170"
    ip-address="192.168.3.100"
    host-group-ids="11,15"
    host-name="some.hostname.local."
    country="XR"
    start-time="2011-03-10T12:31:26Z"
    end-time="2011-03-10T18:06:28Z"
    active="false"
    username="bob">
    <server ip-address="192.168.1.10" name="ms-activedirectory"/>
    <domain name="AD" controller="MSACTDIR"/>
  </user-activity>
  <user-activity ..>
    :
  </user-activity>
  :
</user-activity-list>

```

The `user-activity-list` element contains one or more `user-activity` elements that have the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch Identity appliance that made this observation.	Integer	Required
ip-address	The IP address of the host.	String	Required
host-name	The name of the host.	String	Optional
host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required
country	The country that the host belongs to.	String	Required
start-time	The time at which the login session started.	ISO8601 Date	Required
end-time	The time at which the login session ended.	ISO8601 Date	Optional
active	Indication if the session was active at the time of the request.	Boolean	Required
user-name	The username used for this session,	String	Required

The `user-activity` element contains two sub-elements that describe the authentication server and Windows domain used for the session. The `server` element has the following attributes:

Name	Description	Type	Use
<code>ip-address</code>	The IP address of the server providing the authentication data.	String	Required
<code>name</code>	The name given to the server providing the authentication data.	String	Required

The `domain` element has the following attributes:

Name	Description	Type	Use
<code>name</code>	The name of the Windows domain that the user logged into.	String	Optional
<code>controller</code>	The name of the Windows domain controller associated with the domain that the user logged into.	String	Optional

3.4.2.13 DHCP Lease

The response may contain `dhcp-lease-list` element:

```
<dhcp-lease-list>
  <dhcp-lease
    domain-id="101"
    device-id="391"
    ip-address="192.168.3.100"
    host-group-ids="11"
    host-name="some.hostname.local."
    country="XR"
    start-time="2011-12-11T05:45:57Z"
    end-time="2011-12-18T05:48:13Z"
    active="false">
    <server name="dhcptest1"/>
    <client mac-address="00:ab:cd:ef:12:34" vendor="Acme Inc."/>
  </dhcp-lease>
  <dhcp-lease ..>
    :
  </dhcp-lease>
  :
</dhcp-lease-list>
```

The `dhcp-lease-list` element contains one or more `dhcp-lease` elements that have the following attributes:

Name	Description	Type	Use
<code>domain-id</code>	The ID of the Domain in which the observation was made.	Integer	Required
<code>device-id</code>	The ID of the StealthWatch Identity appliance that made this observation.	Integer	Required
<code>ip-address</code>	The IP address of the host.	String	Required
<code>host-name</code>	The name of the host.	String	Optional

host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required
country	The country that the host belongs to.	String	Required
start-time	The time at which the DHCP lease started.	ISO8601 Date	Required
end-time	The time at which the DHCP lease ended.	ISO8601 Date	Optional
active	Indication if the DHCP lease was active at the time of the request.	Boolean	Required

The `dhcp-lease` element contains two sub-elements that describe the DHCP lease assigning server and the client that requested the lease. The `server` element has the following attributes:

Name	Description	Type	Use
name	The name given to the server assigning the DHCP leases.	String	Required

The `client` element has the following attributes:

Name	Description	Type	Use
mac-address	The MAC address of the host requesting the DHCP lease.	String	Required
vendor	The name of the vendor that has been assigned the MAC address.	String	Optional

3.4.2.14 Host Notes

The response may contain a `host-notes-list` element:

```
<host-note-list>
  <host-note
    domain-id="104"
    ip-address="10.202.4.131"
    host-group-ids="11"
    country="XR",
    time="2011-02-05T20:10:18Z",
    user="admin">This host needs to be tracked.</host-note>
  <host-note ..>
    :
  </host-note>
  :
</host-note-list>
```

The `host-note-list` element contains one or more `host-note` elements that have the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
ip-address	The IP address of the host.	String	Required
host-name	The name of the host.	String	Optional

host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required
country	The country that the host belongs to.	String	Required
time	The time at which the note was added.	ISO8601 Date	Required
user	The name of the user that added the note	String	Required

The text content of the `host-note` element is the actual text of the note.

3.5 getHostInformation

3.5.1 Request

The request takes the form of a `host-information-filter` XML element:

```
<host-information-filter domain-id="101">
  <date-selection>
    :
  </date-selection>
  <device-selection>
    :
  </device-selection>
  <host-selection>
    :
  </host-selection>
  <server-service-list ..>
</server-service-list>
  <server-application-list ..>
</server-application-list>
  <client-service-list ..>
</client-service-list>
  <client-application-list ..>
</client-application-list>
  <operating-system ..></operating-system>
  <alarms ..></alarms>
  <alerts ..></alerts>
  <ci-events ..></ci-events>
</host-information-filter>
```

The `host-information-filter` element has the following attributes:

Name	Description	Type	Use
domain-id	ID of the Domain to be queried.	Integer	Required
max-rows	The maximum number of rows to be returned in the response.	Integer	Optional Default of 2000

The following sections describe the sub-elements of the `host-information-filter`. These sub-elements are optional and must appear in the order described above.

3.5.1.1 Date and Time Filtering

The request may, optionally, filter the returned records based on time:


```
<date-selection>
  :
</date-selection >
```

The `date-selection` element must contain one of the following sub-elements:

- `day-range-selection`
See 4.1.4 for more information.

3.5.1.2 Device Filtering

The request may, optionally, filter the returned records based on the associated device or devices:

```
<device-selection>
  :
</device-selection >
```

The `device-selection` element must contain one of the following sub-elements:

- `device-list-selection`
See 4.2.1 for more information.

3.5.1.3 Host Filtering

The request may, optionally, filter the returned records based on the associated host or hosts, Host Groups, VM servers, VMs, IP Address Ranges:

```
<host-selection>
  :
</host-selection >
```

The `host-selection` element must contain one of the following sub-elements:

- `host-group-selection`
See 4.3.1 for more information.
- `ip-address-range-selection`
See 4.3.2 for more information.
- `ip-list-selection`
See 4.3.3 for more information.
- `vm-list-selection`
See 4.3.5 for more informatrion
- `host-pair-selection`
See 4.3.6 for more information.

3.5.1.4 Service Filtering

The request may, optionally, filter the returned records based on the TCP/UDP services observed for a host as a Client and/or Server

```
<server-service-list operator="AND">
  <profiled-service-list>
    <profiled-service profile-index="93" />
    <profiled-service profile-index="76" />
  </profiled-service-list>
  <custom-service-list>
    <custom-service protocol="tcp" port-number="123-456" />
    <custom-service protocol="udp" port-number="100-102" />
  </custom-service-list>
</server-service-list>
```

```

        </custom-service-list>
    </server-service-list>
    <client-service-list operation="OR">
        <profiled-service-list>
            <profiled-service profile-index="93" />
            <profiled-service profile-index="76" />
        </profiled-service-list>
        <custom-service-list>
            <custom-service protocol="tcp" port-number="123-456" />
            <custom-service protocol="udp" port-number="100-102" />
        </custom-service-list>
    </client-service-list>

```

The `server-service-list` and `client-service-list` elements contain the following attributes:

Name	Description	Type	Use
operator	Specifies how a host is matched to the specified services.	Enumeration of "AND" or "OR"	Required

The `server-service-list` and `client-service-list` contains 2 list elements that specify the services of interest in one of two ways.

The `profiled-service-list` element contains `profiled-service` elements. The element specifies a service as defined in the Service Definitions for the Domain and contains the following attributes:

Name	Description	Type	Use
profile-index	The index as specified in the Service Definitions for the Domain.	Integer	Required

The `custom-service-list` element contains `custom-service` elements. The element specifies a service using the protocol and port/port-range and contains the following attributes:

Name	Description	Type	Use
protocol	The protocol of the service.	Enumeration of "tcp" or "udp"	Required
port-number	The port/port-range associated with this service. e.g. "8080", "100-200"	String	Required

3.5.1.5 Protocol Filtering

Protocol filtering is now done with the `profiled-service` element, instead of a separate XML tag.

For example, in order to add a filter by protocol of 4, add the constant 60000 to the raw protocol number to get 60004 for the `profile-index` of the `profiled-service` element.

To filter by ICMP type, you add the constant 60256 to the raw ICMP type. See 4.7 for a list of ICMP Types.

3.5.1.6 Operating System Filtering

The request may, optionally, filter the returned records based on the operating system that the host is using:

```
<operating-system operator="AND">503331,1493595250</operating-system >
```

The `operating-system` elements contain the following attributes:

Name	Description	Type	Use
operator	Specifies how a host is matched to the specified OSs.	Enumeration of "AND" or "OR"	Required

The `operating-system` element simply contains a comma-separated list of the operating system codes of interest.

NOTE: This constraint should only be used if the device selected in the `device-selection` is a FlowCollector for sFlow appliance.

3.5.1.7 Alarm Filtering

The request may, optionally, filter the returned records based on the type of Alarms that have been active for a host:

```
<alarms operator="AND">1,20,7</alarms>
```

The `alarms` elements contain the following attributes:

Name	Description	Type	Use
operator	Specifies how a host is matched to the specified Alarm types.	Enumeration of "AND " or "OR "	Required

The `alarms` element simply contains a comma-separated list of the Alarm type IDs of interest. See 4.5 for more information.

3.5.1.8 Alert Filtering

The request may, optionally, filter the returned records based on the type of Alerts that have been active for a host:

```
<alerts>2,9,27</alarms>
```

The `alerts` elements contain the following attributes:

Name	Description	Type	Use
operator	Specifies how a host is matched to the specified Alert types.	Enumeration of "AND" or "OR"	Required

The `alerts` element simply contains a comma-separated list of the Alert type IDs of interest. See **Error! Reference source not found.** for more information.

3.5.1.9 CI Event Filtering

The request may, optionally, filter the returned records based on the type of CI Events that have been active for a host:

```
<ci-events>33,37,43</ci-events>
```

The `ci-events` elements contain the following attributes:

Name	Description	Type	Use
operator	Specifies how a host is matched to the specified CI Event types.	Enumeration of "AND " or "OR"	Required

The `ci-events` element simply contains a comma-separated list of the CI Event type IDs of interest. See 4.6 for more information.

3.5.2 Response

The response takes the form of a `host-information-list` element that contains zero or more `host-information` elements:

```
<host-information-list>
  <host-information
    domain-id="102"
    device-id="104"
    ip-address="10.202.10.20"
    host-group-ids="11"
    host-name="somehostname.something.com"
    country="XR"
    time="2011-08-11T20:19:34Z"
    mac-address="00:0b:db:08:a8:79">
    <service-profile-status>
      :
    </service-profile-status>
    <application-activity>
      :
    </application-activity>
    <os>..</os>
    <traffic>
      :
    </traffic>
    <total-traffic ../>
    <high-traffic ../>
    <low-traffic ../>
    <concern-index ../>
    <target-index ../>
    <file-sharing-index ../>
    <new-flows-initiated ../>
    <new-flows-served ../>
    <max-flows-initiated ../>
    <max-flows-served ../>
    <syms-received ../>
    <syms ../>
    <udp ../>
    <icmp ../>
    <ci-events> . . </ci-event>
    <closest-interface ../>
    <interface-list
```

```

        :
        </interface-list>
    </host-information>
<host-information>
    :
    </host-information>
    :
</host-information-list>

```

The `host-information` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain to which this host belongs.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
ip-address	The IP address of the host.	String	Required
host-name	The name of the host.	String	Optional
country	The country that the host belongs to.	String	Required
host-group-ids	The IDs of the Host Groups that the host belongs to.	String	Required
vserver-id	The VM server id on which this host exists.	Integer	Optional
vserver-ip-address	The VM server ip-address on which this host exists.	String	Optional
vserver-name	The VM server name on which this host exists.	String	Optional
vmachine-id	The virtual machine id associated with the host.	Integer	Optional
vmachine-name	The virtual machine name associated with the host.	String	Optional
time	The time associated with this observation	ISO8601 Date	Required
mac-address	The MAC address observed for this host.	String	Optional.

The optional sub-elements contains various information regarding the behavior of the host during the time specified in the filter.

3.5.2.1 Service Profile

The response may contain a `service-profile-status` element that describes the services that have been observed for the host as either a Server or Client:

```

<service-profile-status>
    <server>1:S16,S22</server>
    <client>1:S12,S23,S27,S80</client>
</service-profile-status>

```

See 4.4 for details of the format.

3.5.2.2 Application Activity

The response may contain an `application-activity` element that describes the applications that have been observed for the host as either a Server or Client:

```
<application-activity>
  <server>,169,</server>
  <client>,51,171,169,184,168,81,175,39,53,41,44,</client>
</application-activity>
```

The server or client sub-elements simply contain a comma-separated list of the application-ids as defined in the Services and Applications Configuration Dialog,

3.5.2.3 Alarms

The response may contain an `alarms` element that describes the alarms that have been observed for the host:

```
<alarms>24,32</alarms>
```

The `alarms` element simply contains a comma-separated list of the host alarm ids. See 4.5 table for list of valid alarm ids

3.5.2.4 Alerts

The response may contain an `alerts` element that provides the alerts that have been observed for the host:

```
<alerts>5,22,28</alerts>
```

The `alerts` element simply contains a comma-separated list of the alert ids. See the **Error! Reference source not found.** table for list of valid alert ids.

3.5.2.5 Operating System

The response may contain an `os` element that describes the Operating Systems that have been observed for the host:

```
<os>1897979539</os>
```

NOTE: This element may only be present if a FlowCollector for sFlow appliance made the observation.

3.5.2.6 Traffic Statistics

The response will contain a `traffic` element that describes the inbound and outbound traffic observed for the host:

```
<traffic>
  <in bytes="281869267" packets="1955487" max="64720"></in>
  <out bytes="338649938" packets="2299743" max="64760"></out>
</traffic>
```

NOTE: This element may only be present if an FlowCollector for sFlow appliance made the observation.

The `traffic` element contains an `in` and `out` element that contains the following attributes:

Name	Description	Type	Use
bytes	The total number of payload bytes inbound/outbound to the host during the day.	Long	Required
packets	The total number of IP packets inbound/outbound to the host during the day.	Long	Required
max	The maximum observed inbound/outbound traffic rate (bits per second) during the day.	Integer	Required

3.5.2.7 Policy Statistics

The response will contain a number of elements that describe the statistics that are tracked with respect to a number of the alarms:

```

<total-traffic max="620519205"/>
<data-loss max="1262"/>
<high-traffic max="126212" average="84379"/>
<low-traffic max="3874" average="84379"/>
<concern-index max="0"/>
<target-index max="0"/>
<file-sharing-index max="0"/>
<new-flows-initiated max="0" average="0"/>
<new-flows-served max="0" average="0"/>
<max-flows-initiated max="0" average="0"/>
<max-flows-served max="0" average="0"/>
<syms-received max="0" average="0"/>
<syms max="0" average="0"/>
<udp max="0" average="0"/>
<icmp max="0" average="0"/>

```

Each element may contain the following attributes:

Name	Description	Type	Use
max	The maximum value for that statistic observed during the day.	Long	Required
average	The mean value for that statistic observed during the day	Long	Optional

The following table describes the statistics tracked by each element for the day:

Element Name	Description	Units
total-traffic	Amount of traffic in both directions for the host for the day.	Bytes
high-traffic	Highest rate of traffic in both directions for the host for a period of time.	Bits per second
data-loss	The cumulative amount of suspected data loss by host.	Bytes
low-traffic	Lowest rate of traffic in both directions for the host for a period of time.	Bits per second
concern-index	Concern index value for the host.	Points
target-index	Target index value for the host.	Points

file-sharing-index	File sharing index value for the host.	Points
new-flows-initiated	Highest number of new flows initiated in a 5-minute period by the host.	Count
new-flows-served	Highest number of new flows served (initiated by another host) in a 5-minute period by the host.	Count
max-flows-initiated	Highest number of active flows initiated by the host, measured every 5 minutes.	Count
max-flows-served	Highest number of active flows served (initiated by another host) by the host, measured every 5 minutes.	Count
syns-received	Rate of SYN packets inbound in a 5-minute period to the host.	Packets per 5 minutes
syns	Rate of SYN packets outbound in a 5-minute period to the host.	Packets per 5 minutes
udp	Rate of UDP packets outbound in a 5-minute period by the host.	Packets per 5 minutes
icmp	Rate of ICMP packets outbound in a 5-minute period by the host.	Packets per 5 minutes

3.5.2.8 Concern Index Events

The response may contain a `ci-event` element. This is a comma-separated list of ci-events that contributed to the Concern Index points.

```
<ci-events>
  Addr_Scan/udp, Suspect_UDP_Activity/udp, ICMP_Port_Unreach,
</ci-events>
```

3.5.2.9 Exporters

The response may contain the following elements:

```
<closest-interface
  domain-id="102"
  device-id="104"
  exporter-ip="10.202.4.72"
  if-index="1"
  confidence="98/>
<interface-list>
  <interface
    domain-id="102"
    device-id="104"
    exporter-ip="10.202.4.72"
    if-index="1"/>
  <interface ../>
    :
</interface-list>
```

The `closest-interface` element contains the following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required

device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
exporter-ip	The IP address of the exporter that observed this host.	String	Required
if-index	The index number of the Interface that passed traffic for this host.	Integer	Required
confidence	The confidence level, in percent, with the closest interface determination.	Integer	Required

The `interface-list` element contains one or more `interface` elements that each have the flow following attributes:

Name	Description	Type	Use
domain-id	The ID of the Domain in which the observation was made.	Integer	Required
device-id	The ID of the StealthWatch FlowCollector appliance that made this observation.	Integer	Required
exporter-ip	The IP address of the exporter that observed this host.	String	Required
if-index	The index number of the Interface that passed traffic for this host.	Integer	Required

3.6 getHostGroups

This Web Services request allows the user to get the current Host Group structure for a given Domain.

3.6.1 Request

The request takes the form of a `domain` XML element:

```
<domain id="115" />
```

The `domain` element contains the single `id` attribute that specifies that domain of interest.

3.6.2 Response

The response takes the form of a `host-group-tree` element:

```
<domain id="115">
  <host-group-tree>
    <inside-hosts>
      <host-group id="23" name="Host Group A">
        <ip-address-ranges>10.202.</ip-address-ranges>
        <ip-address-ranges>10.203.</ip-address-ranges>
        :
      <host-group id="24" name="Host Group A1">
        <ip-address-ranges>...
        :
      </host-group>
      :
    </host-group>
    :
  </inside-hosts>
</domain>
```

```

<outside-hosts>
  <host-group id="19" name="AOL IM">
    <ip-address-ranges>64.12.24-26.</ip-address-ranges>
    <ip-address-ranges>64.12.28-29.</ip-address-ranges>
    :
  </host-group>
</outside-hosts>
<host-group id="62001" name="Command & Control Servers" />
<host-group id="65" name="Top-Level Host Group-1">
  <ip-address-ranges>32.12.24-26.</ip-address-ranges>
  <ip-address-ranges>32.12.28-29.</ip-address-ranges>
  :
</host-group>
</host-group-tree>
</domain>

```

The `host-group-tree` element must contain the `inside-hosts` and `outside-hosts` elements. The `host-group-tree` will also contain a `host-group` element named "Command & Control Servers". These elements may then contain a nested tree of `host-group` elements.

The attributes for the `inside-hosts` element and the `outside-hosts` element are the same as the `host-group` element. These attributes are omitted in the sample above for brevity.

The top-level host groups are `host-group` elements that come after the `host-group` element named "Command & Control Servers."

3.7 setHostGroups

This call allows the user to replace the current host group structure for a given domain.

3.7.1 Request

The request takes the form of a `domain` element:

```

<domain id="115">
  <host-group-tree>
    <inside-hosts>
      <host-group id="23" name="Host Group A">
        <ip-address-ranges>10.202.</ip-address-ranges>
        <ip-address-ranges>10.203.</ip-address-ranges>
        :
        <host-group id="24" name="Host Group A1">
          <ip-address-ranges>...
          :
        </host-group>
        :
      </host-group>
      :
    </inside-hosts>
    <outside-hosts>
      <host-group id="19" name="AOL IM">
        <ip-address-ranges>64.12.24-26.</ip-address-ranges>
        <ip-address-ranges>64.12.28-29.</ip-address-ranges>
        :
      </host-group>
    </outside-hosts>
    <host-group id="65" name="Top-Level Host Group-1">
      <ip-address-ranges>32.12.24-26.</ip-address-ranges>
      <ip-address-ranges>32.12.28-29.</ip-address-ranges>
      :
    </host-group>
  </host-group-tree>
</domain>

```

```
    </host-group-tree>  
</domain>
```

The `domain` element must contain the `id` attribute to specify the Domain of interest. The domain specified must already exist.

The `host-group-tree` element must then follow. The `host-group-tree` element must contain the `inside-hosts` and `outside-hosts` elements. These elements may then contain a nested tree of `host-group` elements.

NOTE: Host Group IDs must be larger than 1 and less than 60000. Any Host Groups specified with IDs outside of this range will be ignored.

NOTE: The Countries host group will not be replaced if this call is made. In addition, if the Command & Control Servers host group exists in the tree, it will be replaced.

WARNING: Host Groups statistics are stored by using the 'id' as a key. When using the `setHostGroups` Web Service call, do not change the 'id' number of existing host groups because doing so could cause access to historical data for those groups to be inhibited. If 'id' numbers are reassigned from one group to another, retrieval of historical data for the group may contain records from the host group to which the 'id' was previously assigned.

3.7.2 Response

The response will simply echo the request providing that the call has successfully completed. It will include all attributes showing the defaults taken.

3.8 updateExporters

3.8.1 Request

The request takes the form of a `domain` element:

```
<domain id="101">  
  <swa-list>  
    <swa id="415">  
      <exporter-list auto-add="true">  
        <exporter ip="10.9.1.1" exporter-type="flow-sensor">  
          <snmp>  
            :  
          </snmp>  
          <interface  
            if-index="2"  
            name="if-1"  
            description="if-1"  
            speed-in="1000000000"  
            speed-out="1000000000"  
            threshold-in="90"  
            threshold-out="90" />  
          <interface .. />  
          :  
        </exporter>  
      </exporter-list>  
    </swa>  
  
    <swa id="416">  
      :  
    </swa>  
    :  
  </swa-list>
```

```
</domain>
```

The `domain` element must contain the `id` attribute to specify the Domain of interest.

The `swa-list` element should contain a list of `swa` elements that specify, using the `id` attribute, the StealthWatch FlowCollector devices to be configured.

Each `swa` element should contain an `exporter-list` element that has the following attributes:

Name	Description	Type	Use
auto-add	Indicates if the StealthWatch FlowCollector for sFlow should accept data from any exporter (true) or only those specified (false).	Boolean	Optional

The `exporter-list` element contains a list of `exporter` elements that specify, using the `ip` element, which exporters are to be updated or added. The `exporter` element has the following attributes:

Name	Description	Type	Use
ip	IP Address of the exporter to be updated	IP Address	Required
exporter-type	Specifies the type of exporter. Valid values are: 'exporter', 'flowsensor'	String	Optional
Username	Username for communication credentials, if exporter-type='flowsensor'.	String	Optional
Password	Password for communication credentials, if exporter-type='flowsensor'	String	Optional
hybrid-pair-ip	IP Address of the hybrid pair, if exporter-type='exporter'.	IP Address	Optional
ignore-v5-egress	Ignore egress values when computing interface traffic statistic, if exporter-type='exporter'.	Boolean	Options

The `exporter` element may contain a `snmp` element that specifies if and how the SMC should poll the exporter using the SNMP protocol. This element can take one of 2 forms:

A reference to an SNMP configuration already in the system:

```
<snmp enabled="true">
  <snmp-configuration-ref name="Device Profile #1"/>
</snmp>
```

or an inline SNMP configuration to be used by this exporter alone:

```
<snmp enabled="true">
  <snmp-configuration
    name="SNMP Config A"
    port="161"
    version="2"
    polling-interval="5"
```

SMC Web Services Programming Guide

```

community="public"
use-ifXTable="true"
use-catos-mib="false"
username="user1"
auth-password="password1"
priv-password="password2"
security-level="0"
auth-method="0"
priv-method="0" />
</snmp
>

```

Name	Description	Type	Use
name	The name given to the configuration	String	Required
port	The UDP port that the SNMP requests should be sent.	Short	Optional. Default is "161".
version	The version of the SNMP protocol to use. "1" = SNMP v1 "2" = SNMP v2c "3" = SNMP v3 Default is SNMP v1.	"1", "2" or "3"	Optional. Default is "1".
polling-interval	The number of minutes between each poll. ("0" corresponds to never poll)	Integer	Mandatory
community	The community string. Used in SNMP v1 and 2c only.	String	Optional
use-if-Xtable	Indicates if the if-Xtable MIB should be queried on the exporter.	Boolean	Optional. Default is "false"
use-catos-mib	Indicates if the CatOS MIB should be queried on the exporter.	Boolean	Optional. Default is "false"
username	USM user name. Used in SNMP v3 only.	String	Optional
auth-method	USM authentication protocol. "0" = MD5 "1" = SHA Used in SNMP v3 only.	Integer	Optional
priv-method	USM privacy protocol. "0" = DES "1" = 3DES "2" = AES 128 "3" = AES 192 "4" = AES 256 Used in SNMP v3 only.	Integer	Optional
auth-password	USM authentication key. Used in SNMP v3 only.	String	Optional
priv-password	USP privacy key. Used in SNMP v3 only.	String	Optional

The `exporter` element may then contain a number of `interface` elements that represent the interfaces to be updated/added. These elements contain the following attributes:

Name	Description	Type	Use
<code>if-index</code>	The interface ID or Index.	Integer	Mandatory
<code>name</code>	A string name for the interface.	String	Optional
<code>description</code>	A string description for the interface.	String	Optional
<code>speed-in</code>	The inbound speed of the interface in bits per second.	Integer	Optional
<code>speed-out</code>	The outbound speed of the interface in bits per second.	Integer	Optional
<code>threshold-in</code>	The inbound threshold of the interface. If traffic rises above this percentage of inbound speed an "Exporter Utilization Inbound Exceeded" alarm is generated.	Percent	Optional
<code>threshold-out</code>	The outbound threshold of the interface. If traffic rises above this percentage of outbound speed an "Exporter Utilization Outbound Exceeded" alarm is generated.	Percent	Optional

3.8.2 Response

The response is empty.

3.9 removeExporters

3.9.1 Request

The request takes the form of a `domain` element:

```
<domain id="101">
  <swa-list>
    <swa id="415">
      <exporter-list>
        <exporter ip="10.9.1.1" />
        :
      </exporter>
    </exporter-list>
  </swa>
  <swa id="416">
    :
  </swa>
  :
</swa-list>
</domain>
```

The `domain` element must contain the `id` attribute to specify the Domain of interest.

The `swa-list` element should contain a list of `swa` elements that specify, using the `id` attribute, the StealthWatch FlowCollector devices to be configured.

The `exporter-list` element contains a list of `exporter` elements that specify, using the `ip` element, which exporters are to be removed.

The `exporter` element contains the following attributes (removeExporters required attribute):

Name	Description	Type	Use
<code>ip</code>	IP Address of the exporter	IP Address	Mandatory

3.9.2 Response

The response is empty.

3.10 updateExporterSNMPConfiguration

3.10.1 Request

The request takes the form of a `domain` element:

```
<domain id="101">
  <snmp-configuration-list timeout="5000" retries="3">
    <snmp-configuration
      name="SNMP Config A"
      port="161"
      version="2"
      polling-interval="5"
      community="public"
      use-ifXTable="true"
      use-catos-mib="false"
      username="user1"
      auth-password="password1"
      priv-password="password2"
      security-level="0"
      auth-method="0"
      priv-method="0" />
    :
  </snmp-configuration-list>
</domain>
```

The `domain` element must contain the `id` attribute to specify the Domain of interest.

The `domain` element contains a `snmp-configuration-list` element. The `snmp-configuration-list` element has the following attributes:

Name	Description	Type	Use
<code>default-configuration-name</code>	The name of the SNMP configuration settings that the SMC will use when querying the Exporter when the default SNMP configuration is specified.	String	Optional
<code>time-out</code>	The amount of time in milliseconds that the SMC waits when querying an exporter before aborting the attempt.	Integer	Optional, Default is "5000"

SMC Web Services Programming Guide

retries	The number of attempts that the SMC makes after the first attempt to query an exporter fails.	Integer	Optional, Default is "3"
---------	---	---------	--------------------------

The `snmp-configuration-list` element contains a list of `snmp-configuration` elements. Then `snmp-configuration` element has the following attributes:

Name	Description	Type	Use
name	The name given to the configuration	String	Required
port	The UDP port that the SNMP requests should be sent.	Short	Optional. Default is "161".
version	The version of the SNMP protocol to use. "1" = SNMP v1 "2" = SNMP v2c "3" = SNMP v3 Default is SNMP v1.	"1", "2" or "3"	Optional. Default is "1".
polling-interval	The number of minutes between each poll. ("0" corresponds to never poll)	Integer	Mandatory
community	The community string. Used in SNMP v1 and 2c only.	String	Optional
use-if-Xtable	Indicates if the if-Xtable MIB should be queried on the exporter.	Boolean	Optional. Default is "false"
use-catos-mib	Indicates if the CatOS MIB should be queried on the exporter.	Boolean	Optional. Default is "false"
username	USM user name. Used in SNMP v3 only.	String	Optional
auth-method	USM authentication protocol. "0" = MD5 "1" = SHA Used in SNMP v3 only.	Integer	Optional
priv-method	USM privacy protocol. "0" = DES "1" = 3DES "2" = AES 128 "3" = AES 192 "4" = AES 256 Used in SNMP v3 only.	Integer	Optional
auth-password	USM authentication key. Used in SNMP v3 only.	String	Optional
priv-password	USP privacy key. Used in SNMP v3 only.	String	Optional

3.10.2 Response

The response is empty.

3.11 addHostGroup

This Web Services request adds a new host group. The new host group may be added as any of the following types of host groups:

- Top-level host group
- Sub-host group under Inside Hosts or Outside Hosts
- Sub-host group to any existing host group, except for the following host groups:
 - Catch All
 - Command & Control Servers
 - Countries.

3.11.1 Request

The request takes the form of a `host-group` element:

```
<host-group domain-id="101" id="1" ...>
  <ip-address-ranges>10.201.3.0-10</ip-address-ranges>
  <ip-address-ranges>10.202.</ip_address-ranges>
  :
</host-group>
```

The `host-group` element has the following attributes:

Name	Description	Type	Use
id	ID of the Host Group of interest	Integer	Optional
domain-id	ID of the Domain of interest	Integer	Required
Name	Name of Host Group	String	Optional
parent-id	ID of the Parent. Omit if adding top-level Host Group	Integer	Optional
host-baselines	Indicates if hosts in this Host Group will have individual policies	Boolean	Optional Default is false
suppress-excluded-services	Allows for disabling CI Events using excluding services	boolean	Optional Default is true
inverse-suppression	Disable Flood alarms and CI Events when a Host in this Host Group is the target	Boolean	Optional Default is true
host-trap	Enable 'trapping' of hosts that scan unused addresses in this Host Groups	Boolean	Optional Default is true

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest.

In order to add a top-level Host Group, omit the `parent-id` attribute.

In order to add a Host Group to the Inside-Hosts, set the `parent-id` to 1.

In order to add a Host Group to the Outside-Hosts, set the `parent-id` to 0.

In order to add a Host Group as a sub-group to another Host Group, use the exported configuration xml file to determine the correct `parent-id` element.

The `ip-address-ranges` element contains a string that represents an IP Address or a range of IP Addresses.

This operation will add, subject to validation, the Host Group as specified in the `host-group` element.

3.11.2 Response

The response will return XML in the same format as the request. Note that the value for the Host Group `id` has been assigned and returned in the response. Any optional elements not entered in the request will be returned in the response showing the default values assigned.

3.12 addHostGroups

This Web Services request adds multiple new host groups. The new host groups may be added as any of the following types of host groups:

- Sub-host group under Inside Hosts or Outside Hosts
- Sub-host group to any existing host group, except for the following host groups:
 - Catch All
 - Command & Control Servers
 - Countries

For memory considerations, we recommend you limit the number of new host groups to 3000 per request.

3.12.1 Request

The request takes the form of a `host-group` element:

```
<sub-group-tree domain-id="101">
  <host-group id="84">
    <host-group domain-id="101" id="1" ...>
      <ip-address-ranges>10.201.3.0-10</ip-address-ranges>
      <ip-address-ranges>10.202.</ip_address-ranges>
      :
    </host-group>
    :
  </host-group>
</sub-group-tree>
:
```

The `sub-host-group` element has the following attributes:

Name	Description	Type	Use
domain-id	ID of the Domain of interest	Integer	Required

The `host-group` element has the following attributes:

Name	Description	Type	Use
id	ID of the Host Group of interest	Integer	Optional
domain-id	ID of the Domain of interest	Integer	Optional
Name	Name of Host Group	String	Optional
parent-id	ID of the Parent. Omit if adding top-level Host Group	Integer	Optional
host-baselines	Indicates if hosts in this Host Group will have individual policies	Boolean	Optional Default is false
suppress-excluded-services	Allows for disabling CI Events using excluding services	boolean	Optional Default is true
inverse-suppression	Disable Flood alarms and CI Events when a Host in this Host Group is the target	Boolean	Optional Default is true
host-trap	Enable 'trapping' of hosts that scan unused addresses in this Host Groups	Boolean	Optional Default is true

The top level `host-group` elements do not need to contain any attributes except an id for a host group that already exists. This will be the parent host group for all the host groups defined within it.

If an `id` attribute contains an id that is not already in use, then the specified id will be used for the new host group. If an `id` attribute contains an id that is already in use, then a new id will be assigned to the new host group.

The `ip-address-ranges` element contains a string that represents an IP Address or a range of IP Addresses.

This operation will add, subject to validation, the Host Groups as specified in the `host-group` elements. A validation error in any host groups will result in the entire file being rejected.

3.12.2 Response

The response will return XML in the same format as the request. Note that the value for the Host Group `id` has been assigned and returned in the response. Any optional elements not entered in the request will be returned in the response showing the default values assigned.

3.13 addHostGroupIPRange

This Web Services request will add IP Address Ranges to an existing Host Group.

3.13.1 Request

The request takes the form of a `host-group` element:

```
<host-group id="34" domain-id="101" ...>
  <ip-address-ranges>10.202.1.<ip-addresses-ranges/>
  <ip-address-ranges>10.203.1.<ip-addresses-ranges/>
  :
</host-group>
```

The `host-group` element for this request accepts the following attributes:

Name	Description	Type	Use
<code>id</code>	ID of the Host Group of interest	Integer	Required
<code>domain-id</code>	ID of the Domain of interest	Integer	Required

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest.

The `host-group` element also contains zero or more `ip-address-ranges` elements.

The `ip-address-ranges` element contains a string that represents an IP Address or a range of IP Addresses.

This operation will add, subject to validation, the Host Group IP Ranges as specified in the `host-group` element.

NOTE: IP address ranges cannot be added to either the Countries or the Command & Control Servers host groups.

3.13.2 Response

The response will return XML for the entire `host-group` element and all its configured `ip-address-ranges`.

3.14 addHostGroupIPRanges

This Web Services request will add IP Address Ranges to multiple existing Host Groups.

3.14.1 Request

The request takes the form of multiple `host-group` elements:

```
<multiple-host-groups>
  <host-group id="34" domain-id="101" ...>
    <ip-address-ranges>10.202.1.</ip-addresses-ranges/>
    <ip-address-ranges>10.203.1.</ip-addresses-ranges/>
    :
  </host-group>
</multiple-host-groups>
```

The `host-group` elements for this request accepts the following attributes:

Name	Description	Type	Use
id	ID of the Host Group of interest	Integer	Required
domain-id	ID of the Domain of interest	Integer	Required

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest.

The `host-group` element also contains zero or more `ip-address-ranges` elements.

The `ip-address-ranges` element contains a string that represents an IP Address or a range of IP Addresses.

This operation will add, subject to validation, the Host Group IP Ranges as specified in the `host-group` elements.

NOTE: IP address ranges cannot be added to either the Countries or the Command & Control Servers host groups.

3.14.2 Response

The response will return XML for the entire `host-group` element and all its configured `ip-address-ranges`.

3.15 removeHostGroup

This Web Service request will remove the Host Group specified by the `host-group` element attributes of `domain-id` and `id`.

3.15.1 Request

The request takes the form of a `host-group` element:

```
<host-group id="34" domain-id="101">
</host-group>
```

The `host-group` element for this request accepts the following attributes:

Name	Description	Type	Use
Id	ID of the Host Group of interest	Integer	Required
domain-id	ID of the Domain of interest	Integer	Required

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest and a `id` attribute to specify the Host Group of interest.

This operation will remove, if present, the Host Group specified by the `domain-id` and `id`. Note that Command & Control Servers and its subordinate host groups cannot be removed.

3.15.2 Response

The response is empty.

3.16 removeHostGroupIPRange

3.16.1 Request

The request takes the form of a `host-group` element:

```
<host-group id="34" domain-id="101">
  <ip-address-ranges>10.202.1.</ip-address-ranges>
  <ip-address-ranges>10.201.2.1</ip-address-ranges>
  :
</host-group>
```

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest and an `id` attribute to specify the Host Group of interest.

This operation will remove, if present, the IP address ranges as specified in the `ip-address-ranges` elements. Note that IP address ranges cannot be removed from host groups subordinate to Command & Control Servers.

3.16.2 Response

The response will return XML for the entire `host-group` element and all its configured `ip-address-ranges`.

3.17 setHostGroupIPRange

3.17.1 Request

The request takes the form of a `host-group` element:

```
<host-group id="34" domain-id="101">
  <ip-address-ranges>"10.202.1."</ip-address-ranges>
  <ip-address-ranges>"10.203.1."</ip-address-ranges>
  :
</host-group>
```

The `host-group` element must contain a `domain-id` attribute to specify the Domain of interest and an `id` attribute to specify the Host Group of interest.

This operation will replace the existing IP address ranges for the Host Group, subject to validation, with those specified in the `ip-address-ranges` elements.

NOTE: IP address ranges cannot be defined for either the Countries or the Command & Control Servers host groups.

3.17.2 Response

The response will return XML in the same format as the request that contains the currently configured IP address ranges for the Host Group.

3.18 getDomain

This Web Services request allows the user to get the current configuration of a Domain as specified by the `id` attribute.

3.18.1 Request

The request takes the form of a `domain` element:

```
<domain id="101" />
```

The `domain` element has the following required attribute:

Name	Description	Type	Use
<code>id</code>	ID of the Domain of interest	Integer	Required

This operation will return subject to validation, the Domain group as specified in the `host-group` element.

3.18.2 Response

The response will return XML in the same format as the request. Note that the value for the Host Group `id` has been assigned and returned in the response. Any optional elements not entered in the request will be returned in the response showing the default values assigned.

3.19 addDomain

This Web Services request will add a new Domain.

3.19.1 Request

The request takes the form of a `domain` element:

```
<domain name="SMC A" reset-hour="4">
  <as-configuration ... />
  <host-group-tree ... />
  <policy-list ... />
  <swa-list ... />
  <external-device-list ... />
  <swa-id-list ... />
  <cisco-ise-list ... />
  <alarm-configuration ... />
  <service-definitions ... />
  <application-definitions ... />
  <intergroup-locking-list ... />
  <snmp-configuration-list ... />
  <group-pair-list ... />
  <map-list ... />
</domain>
```

The sub-elements of the `domain` element are shown above for reference.

For the addDomain request, the following attributes are available:

Name	Description	Type	Use
name	Name of the domain	String	Optional Default is 'Domain_xxx' where xxx is the generated domain id.
reset-hour		Short	Required. Valid values are 0-23. Default is 4.

This operation will add, subject to validation, the Domain. A domain id is automatically assigned.

The sub-elements are discussed below.

3.19.1.1 Autonomous System Number Configuration

The `as-configuration` element contains the `internal-as-numbers` element. This element consists of a comma-separated list of as numbers.

```
<as-configuration>
  <internal-as-numbers>10986,12058,,47896,48148,59274</internal-as-numbers>
</as-configuration>
```

3.19.1.2 Host Group Tree

The `host-group-tree` element consists of the `inside-hosts` element, `outside-hosts` element, and `host-group` elements that are referred to as top-level host groups. Command & Control Servers `host-group` elements in the request will be ignored, but any Command & Control Servers host groups in an existing domain on the SMC will be automatically added to your new domain. Top-level host groups are not identified with either the Inside, Outside, or Command & Control Servers host groups.

See 3.11 for details of the `host-group` element.

3.19.1.3 Policy Configuration

It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.4 SWA Device Configuration

The `swa-list` element should contain a list of `swa` elements that specify the StealthWatch FlowCollector devices to be configured.

3.19.1.5 SWA Identity Device Configuration

The `swa-id-list` element should contain a list of `swa-id` elements that specify the SWA Identity devices to be configured.

```
<swa-id-list>
  <swa-id
    id="2104"
    name="test"
    ip-address="10.202.1.217"
    username="admin"
    password="xxxxxxx"
    port="2393"
  />
</swa-id-list>
```

The `swa-id` element has the following attributes:

Name	Description	Type	Use
id	Auto-assigned when added	Integer	Required
name	User provided name	String	Required
ip-address	User provided ip address	String	Required
username	Name used to authenticate with the SWA Identity appliance	String	Required
Password	Pass used to authenticate with the SWA Identity appliance	String	Required
port	Port number used by the SWA Identity appliance	Integer	Optional

3.19.1.6 Cisco ISE Configuration

The `cisco-ise-list` element contains a list of `cisco-ise` elements that specify the Cisco ISE appliances to be configured. Your license will limit the number of Cisco ISE devices you are allowed to add. Any devices over that limit will be ignored.

```
<cisco-ise-list>
  <cisco-ise
    id="2143"
    name="Cisco ISE"
    ip-address="10.203.6.2"
    username="choward"
    password="xxxxxxx"
    time-zone-id="Africa/Cairo"
  />
</cisco-ise-list>
```

The `cisco-ise` element has the following attributes:

Name	Description	Type	Use
id	Auto-assigned when added	Integer	Required
name	User provided name	String	Required
ip-address	User provided ip address	String	Required
username	Name used to authenticate with the ISE	String	Required

Password	Pass used to authenticate with the ISE	String	Required
time-zone-id	User provided configuration. It will default to "etc/UTC"	String from combo box which is populated with a text file provided by Cisco.	Optional

3.19.1.7 External Devices Configuration

The `external-device-list` element should contain a list of `external-device` elements that specify the external devices to be configured.

```
<external-device-list>
  <external-device id="122"
    name="ISS/RealSecure Test"
    ip-address="10.203.6.6"
    type="realsecure">
    <property-list>
      <property key="value" value="test"/>
      :
      <property... />
    </property-list>
  </external-device>
</external-device-list>
```

The `external-device` element has the following attributes:

Name	Description	Type	Use
id	External device id	Integer	Required
ip-address	User provided name	String	Required
type	Valid values are: realsecure snort syslog	String	Required
name	User provided name	String	Required
property-list	User configured properties dependent on types	Name/Value pair	Optional

3.19.1.8 Alarm Configuration

The `alarm-configuration` element is used to change the severity of the individual alarms and consists of an `alarm-severity` sub-element for each alarm that is to be changed.

```
<alarm-configuration>
  <alarm-severity id="36" value="major" />
  <alarm-severity id="40" value="critical" />
</alarm-configuration>
```

The `alarm-severity` element has the following attributes:

Name	Description	Type	Use
<code>id</code>	ID of alarm type. See 4.5 table for list of alarms and ids.	String	Required
<code>value</code>	Valid values are based on the: critical major minor trivial information	String	Required

3.19.1.9 Service-Definitions

The `service-definitions` element contains 1 sub-elements. The `services` element then contains `service` elements. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.10 Application Definitions

The `applications-definitions` element contains 2 sub-elements: `classification-list` and `application-list`. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.11 Host Locking Configuration

The Host Locking Configuration is defined using the `intergroup-locking-list` element which contains a `group-pair` element. It is recommended to export a domain that contains configuration similar to what you desire, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.12 SNMP Configuration

The `snmp-configuration-list` element contains an `snmp-configuration` sub-element for each configuration needed. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.1.13 Host Group Relationships Configuration

The Host Group Relationship configuration is tightly coupled with the Map configuration. It is recommended to export a domain, then extract the entire sections of this for creating the new domain. Better yet, is to just use the exported XML for your new domain making any changes to the exported XML.

3.19.2 Response

The response will return XML is the same format as the request. Note that the value for the Domain `id` has been assigned and returned in the response. Any optional elements not entered in the request will be returned in the response showing the default values assigned.

3.20 removeDomain

This Web Services request will remove the domain as specified by the supplied `id` attribute of the domain to be removed.

3.20.1 Request

The request takes the form of a `domain` element:

```
<domain id="101" />
```

The `domain` element has the following required attribute:

Name	Description	Type	Use
<code>id</code>	ID of the Domain of interest	Integer	Required

The `domain` element must contain an `id` attribute to specify the Domain of interest.

3.20.2 Response

The response is empty

4 Appendix

4.1 Date & Time Filtering

The general form of date and time filtering in a request filter consists of a `date-selection` element:

```
<date-selection>
  :
</date-selection>
```

The following sections will describe the various constructs that maybe contained within the `date-selection` element.

4.1.1 Time Range Selection

This form of filtering simply matches records that fall between a start and end time:

“Match all records between 10th March 2011 4AM GMT and 10th March 2011 5AM GMT”

```
<date-selection>
  <time-range-selection
    start="2011-03-10T04:00:00Z"
    end="2011-03-10T05:00:00Z"/>
</date-selection>
```

“Match all records after 10th March 2011 4AM GMT”

```
<date-selection>
  <time-range-selection start="2011-03-10T04:00:00Z"/>
</date-selection>
```

“Match all records before 10th March 2011 4AM GMT”

```
<date-selection>
  <time-range-selection end="2011-03-10T04:00:00Z"/>
</date-selection>
```

Notice that if the `start` element is not specified the start time is assumed to be epoch and if the `end` element is not specified the end time is assumed to be the time of the request (“now”).

4.1.2 Time Window Selection

This form of filtering matches all records that fall in a time window of fixed length that ends at the time of the request (“now”):

“Match all records from the last 1 hour”

```
<date-selection>
  <time-window-selection duration="3600000"/>
</date-selection>
```

The `duration` attribute is the size of the time window in milliseconds.

4.1.3 Day Selection

This form of filtering matches all records that fall within a specified day. A day, in this context, runs from the Domain's reset hour to reset hour:

“Match all records from the day (24 hours) starting 10th March 2011 12AM GMT”

```
<date-selection>
  <day-selection start="2011-03-10T00:00:00Z"/>
</date-selection>
```

“Match all records from the day (24 hours) starting 3 days ago”

```
<date-selection>
  <day-selection days-before="3"/>
</date-selection>
```

“Match all records from today”

```
<date-selection>
  <day-selection/>
</date-selection>
```

Note that if either the start or days-before attribute is not specified, the selection is interpreted as between the last reset hour and now (“today”).

4.1.4 Day Range Selection

This form of filtering matches all records that fall within a specified range of days. A day, in this context, runs from the Domains reset hour to reset hour:

“Match all records for the 7 days ending with the day that started 10th March 2011 12AM GMT”

```
<date-selection>
  <day-range-selection last-day="2011-03-10T00:00:00Z" day-count="7"/>
</date-selection>
```

“Match all records for the last 7 day”

```
<date-selection>
  <day-range-selection day-count="7"/>
</date-selection>
```

Notice that if the day start-time is not specified, the selection is interpreted as between the last reset hour and now (“today”).

4.1.5 Active Time Selection

As of this writing, the only SOAP request supporting the active time selection is getSecurityEvents.

Certain data records hold to the concept of being active during some period of time. These records hold this information in a start time and an end time.

When requesting these types of data, it is often useful to specify the time these records were active in the request. Simply wrapping a `time-range-selection`, `time-window selection` or `day-selection` with an `active-time-selection` element does this:

“Match all records that were active between 10th March 2011 4AM GMT and 10th March 2011 5AM GMT”

```
<date-selection>
  <active-time-selection>
    <time-range-selection
      start="2011-03-10T04:00:00Z"
      end="2011-03-10T05:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active after 10th March 2011 4AM GMT”

```
<date-selection>
  <active-time-selection>
    <time-range-selection start="2011-03-10T04:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active before 10th March 2011 4AM GMT”

```
<date-selection>
  <active-time-selection>
    <time-range-selection end="2011-03-10T04:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active in the last 1 hour”

```
<date-selection>
  <active-time-selection>
    <time-window-selection duration="3600000"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active in the day (24 hours) starting 10th March 2011 12AM GMT”

```
<date-selection>
  <active-time-selection>
    <day-selection start="2011-03-10T00:00:00Z"/>
  </active-time-selection>
</date-selection>
```

“Match all records that were active today”

```
<date-selection>
  <active-time-selection>
    <day-selection/>
  </active-time-selection>
</date-selection>
```

4.1.6 First-Last Time Selection

As of this writing, the only SOAP request supporting first-last time selection is getCiEvents.

Requests for data that contain both a start and end time (see 4.1.4) may also filter on these times independently:

“Match all records that started active in the day (24 hours) starting 10th March 2011 12AM GMT and stopped being active in the last 1 hour”

```
<date-selection>
  <first-last-time-selection>
    <first>
      <day-selection start="2011-03-10T00:00:00Z"/>
    </first>
    <last>
      <time-window-selection duration="3600000" />
    </last>
  </first-last-time-selection>
</date-selection>
```

If the first or last elements are not present then the start active or end active times are unconstrained.

4.2 Device Filtering

The general form of device filtering in a request filter consists of a `device-selection` element:

```
<device-selection>
  :
</device-selection>
```

The following sections will describe the various constructs that maybe contained within the `device-selection` element.

4.2.1 Device List Selection

This form of filtering allows the request to list the devices that the response will contain data from:

“Match all records that were observed by devices with IDs 111, 112 and 113”

```
<device-selection>
  <device-list-selection>
    <device device-id="111" />
    <device device-id="112" />
    <device device-id="113" />
  </device-list-selection>
</device-selection>
```

4.2.2 Exporter Selection

This form of filtering allows the request to specify an Exporter of interest:

“Match all records that were observed by the flow exporter 192.168.1.2, that is attached to device 111”

```
<device-selection>
  <interface-list-selection>
    <interface device-id="111" exporter-ip="192.168.1.2" />
  </interface-list-selection>
</device-selection>
```

4.2.3 Interface Selection

The form of filtering allows the request to specify an Interface of interest:

“Match all records that refer to interface #12, on the flow exporter 192.168.1.2, that is attached to device 111”

```
<device-selection>
  <interface-list-selection>
    <interface
      device-id="111"
      exporter-ip="192.168.1.2"
      interface-id="12" />
    </interface-list-selection>
  </device-selection>
```

4.3 Host Filtering

The general form of host filtering in a request filter consists of a `host-selection` element:

```
<host-selection>
  :
</host-selection>
```

The following sections will describe the various constructs that maybe contained within the `host-selection` element.

4.3.1 Host Group Selection

This form of filtering simply matches records that concern hosts in a particular Host Group:

“Match all records that refer to hosts in Host Group #10”

```
<host-selection>
  <host-group-selection host-group-id="10"/>
</host-selection>
```

4.3.2 IP Address Range Selection

This form of filtering matches records that concern hosts that have IP address in some range:

“Match all records that refer to hosts with IP address that start in 10.168.”

```
<host-selection>
  <ip-address-range-selection value="10.168." />
</host-selection>
```

4.3.3 IP Address List Selection

This form of filtering matches records that concern hosts that have one of the listed IP addresses:

“Match all records that refer to hosts with IP addresses 192.168.1.10 and 192.168.1.20”

```
<host-selection>
  <ip-address-list-selection>
    <ip-address value="192.168.1.10" />
    <ip-address value="192.168.1.20" />
  </ip-address-list-selection>
</host-selection>
```

4.3.4 IP Address Selection

This form of filtering matches records that concern the host with the specified IP addresses: This form is used for single host filtering such as needed for Host Snapshot.

“Match all records that refer to the host with IP address 192.168.1.20”

```
<host-selection>
  <ip-address-selection value="192.168.1.10" />
</host-selection>
```

4.3.5 VM Selection

This form of filtering matches records that concern specific VM Hosts and/or hosts on specific VM Servers. This is in the form of the `vm-list-selection` sub-element. The `vm-list-selection` has 2 sub-elements that allow for specifying VM Servers using the `vmserver-list` sub-element, and/or the `vm-list` sub-element for specifying VM Hosts. The `vm-list-selection` element can contain both the `vmserver-list` sub-element and the `vm-list` sub-element

“Match all records that refer to the hosts with vm-id of 55 or vm-server-id of 52”

```
<host-selection>
  <vm-list-selection>
    <vmserver-list>
      <vmserver
        id="52"
        device-id="113"
        server-ip-address="10.202.15.68" />
    </vmserver-list>
    <vm-list>
      <vm
        id="55"
        device-id="113"
        server-ip-address="10.202.15.68" />
    </vm-list>
  </vm-list-selection>
</host-selection>
```

4.3.6 Host Pair Selection

Certain data records refer to 2 hosts and some relationship between them. Examples of the type of data are:

- Flows
- CI Events

An example of this query would be:

“Match all records that refer between host 192.168.1.10 and host 192.168.1.20”

```
<host-pair-selection direction="BETWEEN_SELECTION_1_SELECTION_2">
  <selection-1>
    <ip-address-selection value="192.168.1.10" />
  </selection-1>
  <selection-2>
    <ip-address-selection value="192.168.1.20" />
  </selection-2>
</host-pair-selection>
```

The `host-pair-selection` element may contain a `selection-1` and/or `selection-2` which, in turn, contain a host selection. If either of these elements is unspecified, then they are interpreted as “all hosts”. Possible contents of `selection-1` and `selection-2` are:

- `host-group-selection`
See 4.3.1 for more information.
- `ip-address-range-selection`
See 4.3.2 for more information.
- `ip-address-list-selection`
See 4.3.3 for more information.
- `ip-address-selection`
See 4.3.4 for more information.
- `vm-list-selection`
See 4.3.5 for more information.

The `direction` attribute that has the following possible values:

Name	Description
SELECTION_1_A_SELECTION_2_Z	Hosts that match selection 1 are in role A And Hosts that match selection 2 are in role Z
SELECTION_1_Z_SELECTION_2_A	Hosts that match selection 1 are in role Z And Hosts that match selection 2 are in role A
BETWEEN_SELECTION_1_AND_SELECTION_2	Hosts that match selection 1 are in either role A or Z And Hosts that match selection 2 are in either role A or Z

The roles are defined as follows:

Record	Role A	Role Z
Flow	Client	Server
Alarm	Source	Target
CI Event	Source	Target

4.4 Service Profile Status

The service profile status is encoded into a string format:

```
1:P28,T1 2:S1,S48,U3 3:P2 5:O902/tcp
```

The string is made up of up to five sections separated by a white space. Each section starts with a number (“1”, “2”, “3”, “4”, or “5”) that represents the status, followed by a colon (“.”) and then a comma (“,”) separated list of service description.

The possible states are:

Number	Policy	Observed
1	Explicitly allowed in profile	Observed

SMC Web Services Programming Guide

2	Explicitly allowed in profile	Not Observed
3	Explicitly disallowed in profile	Observed
4	Explicitly disallowed in profile	Not Observed
5	Not specified in profile. Implicitly disallowed.	Observed

The service descriptions start with a single letter code (“S”, “P”, “T”, “U”, “O”) followed by a string that gives further detail.

The possible service codes and details are:

Code	Description	Detail
S	Profiled TCP or UDP Service as described in Service Definitions	Index into Service Definitions e.g. S1, S43
P	Profiled protocol as described in Service Definitions	Index into Service Definitions e.g. P1, P4
T	TCP Range	Index into ranges: 1: ports 0-1024 2: ports 1025-2048 3: ports 2049-4096 4: ports 4097-8192 5: ports 8193-16384 6: ports 16385-32768 7: ports 32769-49152 8: ports 49153-65536 e.g. T1, T8
U	UDP Range	Index into ranges: 1: ports 0-1024 2: ports 1025-2048 3: ports 2049-4096 4: ports 4097-8192 5: ports 8193-16384 6: ports 16385-32768 7: ports 32769-49152 8: ports 49153-65536 e.g. U1, U8
O	Unprofiled service	Port and protocol e.g. 902/tcp, 1000/udp

4.5 Alarm Types

NOTE: Some previously used alarms are now obsolete and no longer listed in this file.

ID	Description
1	Host Lock Violation
5	SYN Flood
6	UDP Flood
7	ICMP Flood

SMC Web Services Programming Guide

8	Packet Flood
9	High Volume Email
10	Mail Relay
11	Spam Source
12	Mail Rejects
13	Watch Port Active
14	New Host Active
15	High Target Index
16	High Total Traffic
17	Max Flows Initiated
18	New Flows Initiated
19	SYNS Received
20	High File Sharing Index
24	Suspect UDP Activity
25	MAC Address Violation
26	Half Open Attack
28	Touched
29	Low Traffic
30	High Traffic
31	Watch Host Active
32	High Concern Index
33	Suspect Long Flow
34	Trapped Host
35	Worm Activity
36	Worm Propagation
37	Max Flows Served
38	New Flows Served
39	Beaconing Host
40	Suspect Data Loss
41	Bot Infected Host - Attempted C&C Activity
42	Bot Infected Host - Successful C&C Activity
43	Bot Command & Control Server
44	Slow Connection Flood
45	Data Exfiltration
46	Command and Control
47	Policy Violation
48	Suspect Quiet Long Flow
49	UDP Received
50	ICMP Received
51	Recon
52	Data Hoarding
53	High DDOS Target Index
54	High DDOS Source Index
55	Port Scan

SMC Web Services Programming Guide

56	Exploitation
57	Anomaly
58	Brute Force Login
59	Talks to Phantoms
60	High SMB Peers
61	SSH Reverse Shell
62	Fake Application Detected
63	Scanner Talking
257	Ping
258	ICMP TimeOut
259	TimeOut UDP
260	TimeOut TCP
261	Reset UDP
262	Reset TCP
263	Bad Flag All
264	Bad Flag SYN FYN
265	Bad Flag Reserved (Sflow Only)
266	Bad Flag RST
267	Bad Flag ACK
268	Bad Flag URG
269	Bad Flag No Flag
271	Stealth Scan UDP
272	Stealth Scan TCP
273	SRC=DES
276	Addr Scan TCP
277	Ping Scan
278	Ping Oversized Packet
281	Frag Pkt Too Short
282	Frag Pkt Too Long
283	Frag Different Sizes
286	Addr Scan UDP
289	ICMP Net Unreachable
290	ICMP Host Unreachable
291	ICMP Protocol Unreachable
292	ICMP Port Unreachable
293	ICMP Frag Needed
294	ICMP SRC Route Failed
295	ICMP Dest Network Unknown
296	ICMP Dest Host Unknown
297	ICMP Src Host Isolated
298	ICMP Dest Net Admin
299	ICMP Dst Host Admin
300	ICMP Net Unreachable TOS
301	ICMP Host Unreachable TOS

SMC Web Services Programming Guide

302	ICMP Comm Admin
303	ICMP Host Precedence
304	ICMP Precedence Cutoff
310	Flow Denied
315	Suspect Data Hoarding
316	Target Data Hoarding
317	Connection From TOR Attempted
318	Connection From TOR Successful
319	Inside TOR Exit Detected
513	Connection to TOR Attempted
514	Connection to TOR Successful
515	Inside TOR Entry Detected
516	Connection To Bogon Address Successful
517	Connection From Bogon Address Successful
518	Connection To Bogon Address Attempted
519	Connection From Bogon Address Attempted
4010	FlowCollector Flow Date Lost
4020	Interface Utilization Exceeded Inbound
4030	Interface Utilization Exceeded Outbound
5010	FlowSensor VE Configuration Error
5011	FlowSensor Traffic Lost
5012	FlowSensor RAID Failure
5013	FlowSensor RAID Rebuilding
5998	FlowSensor Time Mismatch
5999	FlowSensor Management Channel Down
6010	New VM
6020	V-Motion
7001	Relationship High Total Traffic
7002	Relationship High Traffic
7003	Relationship Low Traffic
7004	Relationship Max Flows
7005	Relationship New Flows
7006	Relationship Round Trip Time
7007	Relationship Server Response Time
7008	Relationship TCP Retransmission Ratio
7009	Relationship SYN Flood
7010	Relationship UDP Flood
7011	Relationship ICMP Flood
9021	FlowCollector Data Deleted
9022	FlowCollector Database Unavailable
9023	FlowCollector Database Channel Down
9040	FlowCollector Log Retention Reduced
9050	FlowCollector Exporter Count Exceeded
9051	FlowCollector FlowSensor VE Count Exceeded

SMC Web Services Programming Guide

9052	FlowCollector Flow Rate Exceeded
9100	FlowCollector RAID Failure
9102	FlowCollector RAID Rebuilding
9998	FlowCollector Performance Degraded
9999	FlowCollector Stopped
60000	FlowCollector Time Mismatch
60001	Cisco ISE Management Channel Down
60002	FlowCollector Management Channel Down
60003	SMC RAID Failure
60005	SMC RAID Rebuilding
60007	SMC Disk Space Low
60008	SMC Duplicate Primary
60012	StealthWatch Flow License Exceeded
60013	License Corrupted
60014	Unlicensed Feature
60015	SLIC Channel Down
600016	Identity Channel Down
600017	SMC Failover Channel Down
600018	Identity Concentrator Channel Down

4.6 Security Event Types

4.6.1 In previous versions, these were known as CI Events

NOTE: Some previously used alarms are now obsolete and no longer listed in this file.

ID	Description
1	Host Lock Violation
5	SYN Flood
6	UDP Flood
7	ICMP Flood
8	Packet Flood
9	High Volume Email
10	Mail Relay
11	Spam Source
12	Mail Rejects
13	Watch Port Active
14	New Host Active
15	High Target Index
16	High Total Traffic
17	Max Flows Initiated
18	New Flows Initiated
19	SYNS Received
20	High File Sharing Index

SMC Web Services Programming Guide

24	Suspect UDP Activity
25	MAC Address Violation
26	Half Open Attack
28	Touched
29	Low Traffic
30	High Traffic
31	Watch Host Active
32	High Concern Index
33	Suspect Long Flow
34	Trapped Host
35	Worm Activity
36	Worm Propagation
37	Max Flows Served
38	New Flows Served
39	Beaconing Host
40	Suspect Data Loss
41	Bot Infected Host - Attempted C&C Activity
42	Bot Infected Host - Successful C&C Activity
43	Bot Command & Control Server
44	Slow Connection Flood
45	Data Exfiltration
46	Command and Control
47	Policy Violation
48	Suspect Quiet Long Flow
49	UDP Received
50	ICMP Received
51	Recon
52	Data Hoarding
53	High DDOS Target Index
54	High DDOS Source Index
55	Port Scan
56	Exploitation
57	Anomaly
58	Brute Force Login
59	Talks to Phantoms
60	High SMB Peers
61	SSH Reverse Shell
62	Fake Application Detected
63	Scanner Talking
257	Ping
258	ICMP TimeOut
259	TimeOut UDP
260	TimeOut TCP
261	Reset UDP

SMC Web Services Programming Guide

262	Reset TCP
263	Bad Flag All
264	Bad Flag SYN FYN
265	Bad Flag Reserved (Sflow Only)
266	Bad Flag RST
267	Bad Flag ACK
268	Bad Flag URG
269	Bad Flag No Flag
271	Stealth Scan UDP
272	Stealth Scan TCP
273	SRC=DES
276	Addr Scan TCP
277	Ping Scan
278	Ping Oversized Packet
281	Frag Pkt Too Short
282	Frag Pkt Too Long
283	Frag Different Sizes
286	Addr Scan UDP

4.7 ICMP Types

ID	Description
0	Echo Reply
1	Reserved 1
2	Reserved 2
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Reserved 7
8	Echo Request
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved 19
20	Reserved 20

SMC Web Services Programming Guide

21	Reserved 21
22	Reserved 22
23	Reserved 23
24	Reserved 24
25	Reserved 25
26	Reserved 26
27	Reserved 27
28	Reserved 28
29	Reserved 29
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	Where-Are-You
34	I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	Reserved 39
40	Photuris

5 Examples of Accessing SMC Web Services

Below are some very simplistic examples of using the Web Services API

5.1 Using 'wget'

Note: As of v6.X, the '-auth-no-challenge' must be included as a 'wget' option due to a change to session based authentication by the SMC. Otherwise, a '401 error (unknown authentication scheme)' will result from the SOAP request.

5.1.1 'getDomain' request example

Contents of an example getDomainRequest.xml file:

```
<?xml version="1.0" encoding="UTF-8"?><soapenc:Envelope
xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getDomain>
      <domain id="117"/>
    </getDomain>
  </soapenc:Body>
</soapenc:Envelope>
```

'wget' command syntax in a 'bash' shell context:

```
wget --post-file=getDomainRequest.xml --http-user=admin -ht --auth-no-challenge \
  http-password=xxxxxxx --no-check-certificate -O reponseDomain.xml \
  https://smc1.mydomain.com/smc/swsService/configuration
```

5.1.2 'getHostSnapshot' request

Contents of an example getHostSnapshot.xml file:

```
<?xml version="1.0" encoding="UTF-8"?><soapenc:Envelope
xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getHostSnapshot>
      <host-filter domain-id="117">
        <host-selection>
          <ip-address-selection value="10.203.1.110"/>
        </host-selection>
      </host-filter>
    </getHostSnapshot>
  </soapenc:Body>
</soapenc:Envelope>
```

'wget' command syntax in a 'bash' shell context:

```
wget --post-file=getHostSnapshot.xml --http-user=admin -ht --auth-no-challenge \
  http-password=xxxxxxx --no-check-certificate -O reponseHostSnapshot.xml \
  \ https://smc1.mydomain.com/smc/swsService/hosts
```

5.2 Using 'curl'

5.2.1 'getHostInformation' request

Contents of an example getHostInfo.xml file :

```
<?xml version="1.0" encoding="UTF-8"?><soapenc:Envelope
xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getHostInformation>
      <host-information-filter max-rows="2000" domain-id="117">
        <date-selection>
          <day-range-selection day-count="1"/>
        </date-selection>
      </host-information-filter>
    </getHostInformation>
  </soapenc:Body>
</soapenc:Envelope>
```

'curl' command syntax in a 'bash' shell context:

```
curl --tcp-nodelay -m 1 -o responseHostInfo.xml -u admin:mypassword -k -d@getHostInfo.xml \
https://smc1.mydomain.com/smc/swsService/hosts
```

5.2.2 'getSecurityEvents' request

Contents of an example SecurityEventsReq.xml file :

```
<?xml version="1.0" encoding="UTF-8"?><soapenc:Envelope
xmlns:soapenc="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenc:Body>
    <getSecurityEvents>
      <security-event-filter domain-id="117">
        <host-selection>
          <host-pair-selection direction="BETWEEN_SELECTION_1_SELECTION_2">
            <selection-1>
              <ip-address-list-selection>
                <ip-address value="10.203.1.110"/>
              </ip-address-list-selection>
            </selection-1>
          </host-pair-selection>
        </host-selection>
      </security-event-filter>
    </getSecurityEvents>
  </soapenc:Body>
</soapenc:Envelope>
```

'curl' command syntax in a 'bash' shell context:

```
curl --tcp-nodelay -m 1 -o SecurityEventsReq.xml -u admin:mypassword -k -d@CiEventsReq.xml \
https://smc1.mydomain.com/smc/swsService/security
```

5.3 Using 'python'

5.3.1 'addDomain' request

This simplistic python script uses a file retrieved via a 'getDomain' Web Services call to restore the domain configuration to the SMC.

```

from lxml import etree
import pycurl

def smcRequest(url, request):
    response_file = open("responseAddDomain.xml", "w")
    co = pycurl.Curl()
    co.setopt(co.UNRESTRICTED_AUTH, 1)
    co.setopt(co.URL, url)
    co.setopt(co.POST, 1)
    co.setopt(co.WRITEDATA, response_file)
    co.setopt(co.INFILESIZE, len(request) + 1)
    co.setopt(co.POSTFIELDS, request)
    co.setopt(co.SSL_VERIFYPEER, 0L)
    co.setopt(co.SSL_VERIFYHOST, 0L)
    co.setopt(co.USERPWD, "admin:mypassword")
    try :
        co.perform()
    except :
        print "POST failed"
        exit(1)
    co.close()
    response_file.close()
# tidy up the response for human readability
parsed = etree.parse("responseAddDomain.xml")
response = etree.tostring(parsed, pretty_print = True)
response_file = open("responseAddDomain.xml", "w")
response_file.write(response)
response_file.close()
return(response)

def addDomain(domain_id, domain_file):
# assume the 'domain_file' is from a previous "getDomain" request
header = '<?xml version="1.0" encoding="UTF-8"?>'
    try :
        parsed = etree.parse(domain_file)
        request = header + '\n' + etree.tostring(parsed, pretty_print = True)
    except :
        print "Malformed input file : %s" % domain_file
        exit(1)
    return(request.replace("getDomainResponse", "addDomain"))

def main():
    domainID = 117
    xml = addDomain(domainID, "responseDomain.xml")
    url = "https:smc1.mydomain.com/smc/swsService/configuration"
    response = smcRequest(url, xml)
    print response

if name == " main ":
    main()

```

Index

5-min.....	37	ci-event.....	57
access control.....	6	ci-events.....	37, 53
active.....	44, 45, 46, 48	ci-points.....	29, 30, 31
active time selection.....	79	Cisco ISE Configuration.....	74
active-dest-list.....	41	cisco-ise.....	74
active-source-list.....	41	cisco-ise-list.....	74
active-time-selection.....	15, 28	client.....	22, 24, 45, 48
addDomain.....	72	Client Ports Filtering.....	20
addHostGroup.....	66, 67	client-ports.....	20
addHostGroupIPRange.....	69	client-service-list.....	51
addressing.....	6	closest-interface.....	41, 57
Alarm Configuration.....	75	closest-interface-list.....	41
Alarm Filtering.....	52	community.....	62, 65
alarm types, table.....	85	Concern Index.....	35
alarm-configuration.....	75	Concern Index Events.....	57
alarm-counts.....	43	Concern Index Filtering.....	29
alarm-counts-list.....	42	concern-index.....	56
alarm-list.....	43	confidence.....	41, 58
alarms.....	52, 55	connected.....	39
alarms-counts.....	42	connected-host-group-ids.....	39
alarm-severity.....	75	connected-vm.....	39
alarm-type.....	43	connections.....	22
alerts.....	52, 55	console, Java.....	9
application.....	26	controller.....	47
Application Definitions.....	76	country...23, 30, 33, 35, 44, 45, 46, 48, 49, 54	
application-activity.....	35, 55	current-bps.....	42
application-id.....	8, 22	current-pps.....	42
applications.....	17	current-util.....	42
Applications Filtering.....	17	custom-service.....	51
ascii.....	26	data record types.....	5
as-configuration.....	73	data-loss.....	56
asn.....	23	data-loss-threshold.....	37
ASN filtering.....	19	Date & Time Filtering.....	78
as-numbers.....	19	Date and Time Filtering.....	49
authentication.....	6	date-selection.....	11, 14, 27, 31, 78
auth-method.....	62, 65	day.....	37
auth-password.....	62, 65	day range selection.....	79
auto-add.....	61, 64	day selection.....	79
Autonomous System Number.....	19	day-selection.....	31
Autonomous System Number Configuration... 73		description.....	63
average.....	56	details.....	30, 43
average-bps.....	39, 42	details-list.....	30
average-pps.....	42	device filtering.....	81
avg-rtt.....	39	device list selection.....	81
avg-srt.....	40	device-id, 8, 12, 22, 30, 33, 34, 35, 36, 41, 42, 43, 45, 46, 47, 54, 58	
been-touched.....	36	device-list-selection.....	15, 28, 32
bytes.....	23, 25, 56	device-selection.....	11, 15, 28, 31, 52, 81
bytes-received.....	39	dhcp-lease.....	47, 48
bytes-sent.....	39	dhcp-lease-list.....	47
CI Event Filtering.....	53		

differentiated services code point filtering..... 19

direction.....25, 84

domain..... 47, 58, 60, 63, 64

domain-id 8, 12, 14, 22, 27, 30, 31, 33, 34, 35,
36, 41, 42, 43, 44, 46, 47, 48, 49, 54, 57, 58,
66, 68, 69, 70, 71

dscp.....12, 25

DSCP filtering.....19, 20

dscp-list..... 19

dscp-traffic..... 12

dscp-traffic-filter..... 11

dscp-traffic-list..... 12

duration..... 78

end-time.....44, 45, 46, 48

exclude..... 16, 17, 19, 20

exporter.....61, 64

exporter selection..... 81

exporter-ip.....12, 25, 41, 58

exporter-list.....61, 64

exporters.....40, 41

Exporters.....24, 57

exporter-selection..... 15

exporter-type..... 61

External Devices Configuration..... 75

external-device..... 75

external-device-list..... 75

file-sharing-index..... 57

filter semantics..... 8

fin..... 24

first-last time selection..... 80

first-last-time-selection.....15, 28

first-seen..... 34

flags..... 23

flow.....21, 38

flow-filter.....13, 14

flow-list..... 21

flows..... 38

flowsensor..... 26

getDomain.....72

getFlows..... 13

getHostGroups.....58

getHostInformation.....49

getHostSnapshot.....31

getSecurityEvents..... 27

has-touched..... 36

high-traffic..... 56

high-value.....18, 29

hit-count.....29, 31

Host filtering..... 82

Host Filtering..... 50

Host Group ID..... 60

Host Group Relationships Configuration..... 76

Host Group Selection..... 82

Host Group Tree.....73

Host Locking Configuration..... 76

Host Pair Selection..... 83

host-baselines..... 66, 68

host-filter..... 31

host-group.....59, 66, 68, 69, 70, 73

host-group-id..... 8

host-group-ids..8, 23, 30, 33, 34, 44, 45, 46,
48, 49, 54

host-group-selection..... 50

host-group-tree..... 58, 60, 73

host-information..... 34, 53, 54

host-information-filter..... 49

host-information-list..... 34, 53

host-name.....23, 30, 33, 44, 45, 46, 47, 48, 54

host-note..... 48

host-note-list..... 48

host-notes-list..... 48

host-pair-selection..... 15, 28, 50

host-selection..... 15, 28, 32, 82

host-snapshot..... 32

host-trap..... 66, 68

hybrid-pair-ip..... 61

icmp..... 57

ICMP type..... 16

ICMP Types..... 91

id.....43, 69, 70, 77

identifiers..... 8

if-index..... 12, 25, 41, 58, 63

ignore-v5-egress..... 61

inside-hosts..... 59, 60, 73

interface.....25, 58, 63

Interface Selection..... 81

interface-list..... 23, 24, 58

interface-selection..... 12, 15

interface-status..... 41, 42

intergroup-locking-list..... 76

internal-as-numbers..... 73

inverse-suppression..... 66, 68

ip..... 64

IP address list selection..... 82

IP address range selection..... 82

IP Address Ranges..... 69

IP address selection..... 83

IP protocol..... 16

IP Ranges..... 69, 70

ip-address..23, 30, 33, 34, 44, 45, 46, 47, 48,
54

ip-address-range..... 71

ip-address-ranges.....67, 68, 69, 70, 71

ip-address-range-selection..... 50

ip-address-selection..... 32

ip-list-selection..... 50

Java Web Start..... 9

last-seen..... 34

last-time.....22, 30, 39

low-traffic..... 56

low-value.....18, 29

MAC address..... 34

mac-address..... 23, 34, 45, 48, 54

max..... 56

max-flows-initiated..... 57

max-flows-served..... 57

maximum-bps..... 42

maximum-pps..... 42

maximum-util..... 42

max-rows.....14, 27, 49

max-rtt..... 39

max-srt..... 40

max-ttl..... 25

min-rtt..... 39

min-srt..... 39

min-ttl..... 25

MPLS Labels Filtering.....20, 21

mpls-label..... 22

mpls-labels.....20, 21

name..... 45, 46, 47, 48, 62, 63, 73

nbar..... 26

Network Performance Statistics Filtering..... 18

network-performance..... 18

new-flows-initiated..... 57

new-flows-served..... 57

Operating System..... 55

Operating System Filtering..... 52

operating-system..... 52

operator.....51, 52, 53

order-by..... 14

order-by-desc..... 14

os..... 55

outside-hosts.....59, 60, 73

packet data..... 25

packets.....23, 25, 56

packetshaper..... 26

parent-id.....66, 68

Password..... 61

payload.....23, 26

Payload Filtering..... 20

payload-match-all..... 21

payload-match-any..... 21

payload-not-match-all..... 21

Policy Configuration..... 73

policy statistics..... 56

polling-interval.....62, 65

port.....23, 62, 65

port-number..... 51

ports..... 16, 28

Ports Filtering..... 16

prerequisites..... 5

priv-method..... 62, 65

priv-password..... 62, 65

profiled-service..... 51

profiled-service-list..... 51

profile-index..... 19, 20, 51

protocol.....39, 51

Protocol Filtering..... 51

protocols..... 16

Protocols Filtering..... 16

query..... 21

removeDomain..... 77

remove-duplicates..... 14

removeExporters..... 63

removeHostGroupIPRange..... 70, 71

reset-hour..... 73

response..... 53

retention..... 12

retransmits..... 22

retries..... 65

role..... 39

roles..... 84

rst..... 24

rtt..... 27

security..... 35

Security Event Type Filtering..... 28

security-event..... 30

security-event-filter..... 27

security-event-list..... 29

security-list..... 35

server.....22, 24, 45, 47, 48

server-service-list..... 51

service..... 22, 39

service codes..... 85

Service Filtering..... 50

Service Profile..... 54

service profile status..... 84

Service-Definitions..... 76

service-id..... 22

service-profile-status..... 35, 54

services..... 15

Services Filtering..... 15

services-definitions..... 15

setHostGroupIPRange..... 71

setHostGroups..... 59

snmp..... 61

SNMP Configuration..... 76

snmp-configuration..... 65

snmp-configuration-list..... 64, 65, 76

SOAP..... 6

source..... 30, 43

speed-in.....	63	total-retrans.....	39
speed-out.....	63	total-traffic.....	56
spi.....	8	touched-list.....	35
srt.....	27	traffic.....	17, 18, 36, 55
start-time.....	22, 30, 39, 44, 45, 46, 48	Traffic Statistics Filtering	17
status.....	33	traffic-in.....	12
status-list.....	33	traffic-list.....	36
suppress-excluded-services.....	66, 68	traffic-out.....	12
swa.....	61, 63	transport	6
SWA Devices	73	type.....	30, 44
SWA Identity Device Configuration	74	udp.....	57
swa-id.....	74	updateExporters.....	60
swa-id-list.....	74	updateExporterSNMPConfiguration.....	64
swa-list.....	61, 63, 73	use-catos-mib.....	62, 64, 65
syn.....	23	use-if-Xtable.....	62, 65
syn-ack.....	24	user.....	49
syms.....	57	user-activity.....	44, 45, 46
syms-received.....	57	user-activity-list.....	44, 46
target.....	30, 43	username.....	45, 46, 62, 65
Target Index	35	Username.....	61
target-index.....	56	value.....	34, 35
TCP/UDP service	15	vendor.....	34, 45, 48
threshold.....	35, 37	version.....	62, 65
threshold-in.....	63	Virtual LAN IDs	19
threshold-out.....	63	vlan-id.....	22
time.....	12, 49, 54	vlan-ids.....	19
time range selection	78	vmachine-id.....	23, 54
time window selection	78	vmachine-name.....	23, 54
time-out.....	64	vm-list-selection.....	50
today-list.....	41	vserver-id.....	23, 54
top-level	59, 66	vserver-ip-address.....	23, 54
Total-bytes.....	37	vserver-name.....	23, 54
total-conn.....	39	web service requests	9
Total-data-bytes.....	37	WSDL definition	5
total-hits.....	30	XML	9
Total-loss.....	37	XML message types	5
Total-packets.....	37	XML types	5