



APPENDIX **A**

Cisco Security MARS XML API Reference

This appendix provides resources for creating XML applications that integrate Cisco Security MARS XML data into third-party applications.

XML Schema Overview

The XML schema are written in conformance with the standard World Wide Web Consortium (W3C) XML schema language. A schema by definition, describes all data and data structures required to create your application. Many XML development environments provide enough capability to view the schema in a way that you can identify all components, their relationships, constraints, attributes, annotations, and usage guidelines at a glance. Some applications generate hyperlinked reference documentation. By providing sufficient documentation and annotation tags within the schemas, Cisco supports such documentation generating applications.

[Table A-1](#) lists resources for XML development.

Table A-1 XML Resources

Resource Description	URL
W3C XML Schema standards forum with resource links	http://www.w3.org/XML/Schema
General XML description with resource links	http://en.wikipedia.org/wiki/XML
Online XML Tutorials	http://www.w3schools.com/xml/default.asp

XML Incident Notification Data File and Schema

XML incident notification sends an email notification of an incident with an attached XML data file. The XML data file contains all incident details that can be viewed on the GUI except for Path/Mitigation data. The XML data file can be sent as a plain-text file or as a compressed gzip file. The filename is constructed with the incident ID number, for example `CS-MARS-Incident-13725095.xml`. The compressed version of the same data file would be `CS-MARS-Incident-13725095.xml.gz`

An XML application can be written to parse and extract data from the XML incident notification data file for integration into third-party software, such as a trouble ticketing system, or helpdesk software.

[Table A-2](#) lists the documentation for the Cisco Security MARS XML incident notification feature.

Table A-2 Related XML Incident Notification Documents

Resource Description	Resource Location
Configuring XML incident notification on MARS	Chapter 9, “Sending Alerts and Incident Notifications”
A ZIP file containing the XML incident notification schema	http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.2/technical/reference/xmlnotif.zip
A hyper-linked component reference, generated from the XML incident notification schema	http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.2/technical/reference/xnotidoc.zip
Sample XML incident notification data generated by MARS	Appendix A, “Example A-1

XML Incident Notification Data File Sample Output

[Example A-1](#) is XML incident notification data generated by the events that trigger the rule “CS-MARS Database Partition Usage.”

Example A-1 XML Incident Notification Data File Contents

```
<?xml version="1.0" encoding="UTF-8"?>
<CSMARS-NOTIFICATION>
  <Header>
    <Version>1.0</Version>
    <GenTimeStamp>May 23, 2007 8:13:19 AM PDT</GenTimeStamp>
    <CSMARSHostIpAddr_eth0>10.2.3.48</CSMARSHostIpAddr_eth0>
    <CSMARSHostIpAddr_eth1>192.168.1.110</CSMARSHostIpAddr_eth1>
    <CSMARSHostName>pnmars</CSMARSHostName>
    <CSMARSZoneName />
    <CSMARSVersion>4.2.2</CSMARSVersion>
  </Header>
  <Data>
    <Incident id="287001899">
      <StartTime>May 23, 2007 8:13:09 AM PDT</StartTime>
      <EndTime>May 23, 2007 8:13:10 AM PDT</EndTime>
      <Severity>HIGH</Severity>
      <Session id="286913412">
        <Instance>0</Instance>
        <SessionEndPoints>
          <Source ipaddress="10.3.50.200" />
          <Destination ipaddress="248.64.35.88" />
          <SourcePort>15330</SourcePort>
          <DestinationPort>3890</DestinationPort>
          <Protocol>6</Protocol>
        </SessionEndPoints>
        <Event id="286914062">
          <EventType id="1135" />
          <TimeStamp>May 23, 2007 8:13:09 AM PDT</TimeStamp>
          <ReportingDevice id="128783" />
          <RawMessage>Wed May 23 08:13:09 2007 &lt;134&gt;%PIX-2-106001: Inbound TCP
connection denied from 10.3.50.200/15330 to 248.64.35.88/3890 flags FIN on interface
inside</RawMessage>
          <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
          <EventEndPoints>
            <Source ipaddress="10.3.50.200" />
          </EventEndPoints>
        </Event>
      </Session>
    </Incident>
  </Data>
</CSMARS-NOTIFICATION>
```

```

        <Destination ipaddress="248.64.35.88" />
        <SourcePort>15330</SourcePort>
        <DestinationPort>3890</DestinationPort>
        <Protocol>6</Protocol>
    </EventEndPoints>
    <NATtedEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="248.64.35.88" />
        <SourcePort>15330</SourcePort>
        <DestinationPort>3890</DestinationPort>
        <Protocol>6</Protocol>
    </NATtedEndPoints>
    <FiringEventFlag>true</FiringEventFlag>
    <RuleMatchOffset>1</RuleMatchOffset>
</Event>
<Event id="286913412">
    <EventType id="1135" />
    <TimeStamp>May 23, 2007 8:11:53 AM PDT</TimeStamp>
    <ReportingDevice id="128783" />
    <RawMessage>Wed May 23 08:11:53 2007 &lt;134&gt;%PIX-2-106001: Inbound TCP
connection denied from 10.3.50.200/15330 to 248.64.35.88/3890 flags FIN on interface
inside</RawMessage>
    <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
    <EventEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="248.64.35.88" />
        <SourcePort>15330</SourcePort>
        <DestinationPort>3890</DestinationPort>
        <Protocol>6</Protocol>
    </EventEndPoints>
    <NATtedEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="248.64.35.88" />
        <SourcePort>15330</SourcePort>
        <DestinationPort>3890</DestinationPort>
        <Protocol>6</Protocol>
    </NATtedEndPoints>
    <FiringEventFlag>false</FiringEventFlag>
</Event>
</Session>
<Session id="286914063">
    <Instance>0</Instance>
    <SessionEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="105.74.127.53" />
        <SourcePort>0</SourcePort>
        <DestinationPort>0</DestinationPort>
        <Protocol>0</Protocol>
    </SessionEndPoints>
    <Event id="286914063">
        <EventType id="1137" />
        <TimeStamp>May 23, 2007 8:13:10 AM PDT</TimeStamp>
        <ReportingDevice id="128783" />
        <RawMessage>Wed May 23 08:13:10 2007 &lt;134&gt;%PIX-2-106016: Deny IP spoof
from (10.3.50.200) to 105.74.127.53 on interface inside</RawMessage>
        <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
        <EventEndPoints>
            <Source ipaddress="10.3.50.200" />
            <Destination ipaddress="105.74.127.53" />
            <SourcePort>0</SourcePort>
            <DestinationPort>0</DestinationPort>
            <Protocol>0</Protocol>
        </EventEndPoints>
    </Event>
    <NATtedEndPoints>

```

```

        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="105.74.127.53" />
        <SourcePort>0</SourcePort>
        <DestinationPort>0</DestinationPort>
        <Protocol>0</Protocol>
    </NATtedEndPoints>
    <FiringEventFlag>true</FiringEventFlag>
    <RuleMatchOffset>1</RuleMatchOffset>
</Event>
</Session>
<Session id="286914072">
    <Instance>0</Instance>
    <SessionEndPoints>
        <Source ipaddress="10.3.50.200" />
        <Destination ipaddress="133.67.205.96" />
        <SourcePort>0</SourcePort>
        <DestinationPort>0</DestinationPort>
        <Protocol>6</Protocol>
    </SessionEndPoints>
    <Event id="286914072">
        <EventType id="1139" />
        <TimeStamp>May 23, 2007 8:13:10 AM PDT</TimeStamp>
        <ReportingDevice id="128783" />
        <RawMessage>Wed May 23 08:13:10 2007 &lt;134&gt;%PIX-1-106022: Deny tcp
connection spoof from 10.3.50.200 to 133.67.205.96 on interface inside</RawMessage>
        <FalsePositiveType>NOT_AVAILABLE</FalsePositiveType>
        <EventEndPoints>
            <Source ipaddress="10.3.50.200" />
            <Destination ipaddress="133.67.205.96" />
            <SourcePort>0</SourcePort>
            <DestinationPort>0</DestinationPort>
            <Protocol>6</Protocol>
        </EventEndPoints>
        <NATtedEndPoints>
            <Source ipaddress="10.3.50.200" />
            <Destination ipaddress="133.67.205.96" />
            <SourcePort>0</SourcePort>
            <DestinationPort>0</DestinationPort>
            <Protocol>6</Protocol>
        </NATtedEndPoints>
        <FiringEventFlag>true</FiringEventFlag>
        <RuleMatchOffset>1</RuleMatchOffset>
    </Event>
</Session>
<Rule id="128791">
    <Name>bd</Name>
    <Description>stack and decker</Description>
</Rule>
<NetworkAddressObj id="4164952920">
    <IPAddress>248.64.35.88</IPAddress>
    <MAC />
    <DNSName />
    <DynamicInfo>
        <HostName />
        <MACAddress />
        <AAAUser />
        <EnforcementDeviceAndPort />
        <ReportingDevice />
        <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
        <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
        <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
    </DynamicInfo>
</NetworkAddressObj>
<NetworkAddressObj id="2235813216">

```

```

<IPAddress>133.67.205.96</IPAddress>
<MAC />
<DNSName />
<DynamicInfo>
  <HostName />
  <MACAddress />
  <AAAUser />
  <EnforcementDeviceAndPort />
  <ReportingDevice />
  <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
  <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
  <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
</DynamicInfo>
</NetworkAddressObj>
<NetworkAddressObj id="167981768">
  <IPAddress>10.3.50.200</IPAddress>
  <MAC />
  <DNSName />
  <DynamicInfo>
    <HostName />
    <MACAddress />
    <AAAUser />
    <EnforcementDeviceAndPort />
    <ReportingDevice />
    <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
    <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
    <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
  </DynamicInfo>
</NetworkAddressObj>
<NetworkAddressObj id="1766489909">
  <IPAddress>105.74.127.53</IPAddress>
  <MAC />
  <DNSName />
  <DynamicInfo>
    <HostName />
    <MACAddress />
    <AAAUser />
    <EnforcementDeviceAndPort />
    <ReportingDevice />
    <StartTime>Dec 31, 1969 4:00:00 PM PST</StartTime>
    <EndTime>Dec 31, 1969 4:00:00 PM PST</EndTime>
    <UpdateTime>Dec 31, 1969 4:00:00 PM PST</UpdateTime>
  </DynamicInfo>
</NetworkAddressObj>
<EventTypeObj id="1139">
  <Name>1106022</Name>
  <Description>Denied spoofed packet - different ingress interface</Description>
  <Severity>HIGH</Severity>
  <CVE />
</EventTypeObj>
<EventTypeObj id="1135">
  <Name>1106001</Name>
  <Description>Deny packet due to security policy</Description>
  <Severity>LOW</Severity>
  <CVE />
</EventTypeObj>
<EventTypeObj id="1137">
  <Name>1106016</Name>
  <Description>Denied IP spoof</Description>
  <Severity>MEDIUM</Severity>
  <CVE />
</EventTypeObj>
<DeviceObj id="128783">
  <Name>pixie</Name>

```

```

        <NetBiosName />
        <DefaultGateway>0.0.0.0</DefaultGateway>
        <OperatingSystem id="0" />
    </DeviceObj>
</Incident>
</Data>
</CSMARS-NOTIFICATION>

```

XML Incident Notification Schema

The XML incident notification schema document (csmars-incident-notification-v1_0.xsd) can be downloaded from the the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.2/technical/reference/xml_notif.zip

Usage Guidelines and Conventions for XML Incident Notification

All XML incident notification elements are defined in the XML incident notification schema. A WinZip archive containing a component reference document generated from the schema is available for your convenience at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.2/technical/reference/xnot_idoc.zip

You can generate a similar document with the application of your choice, or view components, their relationships, constraints, attributes, annotations, and usage guidelines within your XML development environment.

MARS uses a best effort approach to create XML incident notification data. If an error occurs during data compilation, MARS does not stop the process, but sends the data, even if it is partial. Validating the data file against the schema would result in errors for these cases.

The following conventions are observed for XML incident notification data:

- Character encoding is Unicode Transformation Format 8 (UTF-8)
- The reported time zone would be the time zone of the local controller reporting the incident
- Raw messages from reporting devices are XML-escaped in the data file. Your XML parser should be able to unescape XML data.
- If there is no value for an element available from MARS, the element is included in the data file as an empty node. For instance, a DNS name may not be available for a device.
- All date formats are **Mmm dd, yyyy hh:mm:ss AM TZD**
 - **Mmm** is the month (Jan, Feb, Mar. . . Dec)
 - **dd** is the day (1–9, 10–31)
 - **yyyy** is the year (0000–9999)
 - **hh:mm:ss** is hours, minutes, seconds
 - hh** are 1–9, 10–12
 - mm** are 00–60
 - ss** are 00–60
 - **AM** or **PM**
 - **TZD** is time zone designator (PDT, PST, MDT, MST, etc.)