

# OMA DM: VPN Client Management Object Specification

Version 1.0; April 30, 2007

OMA Device  
Management

**NOKIA**

Copyright © 2008 Nokia Corporation. All rights reserved.

Nokia and Forum Nokia are trademarks or registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

#### Disclaimer

The information in this document is provided “as is,” with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. This document is provided for informational purposes only.

Nokia Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to implementation of information presented in this document. Nokia Corporation does not warrant or represent that such use will not infringe such rights.

Nokia Corporation retains the right to make changes to this document at any time, without notice.

#### License

A license is hereby granted to download and print a copy of this document for personal use only. No other license to any other intellectual property rights is granted herein.

## Contents

<b>1</b>	<b>Introduction</b> .....	<b>5</b>
1.1	Supported management operations.....	5
1.2	Supported manageable data.....	5
1.3	Documentation conventions.....	5
<b>2</b>	<b>VPN management object nodes</b> .....	<b>6</b>
2.1	List of management nodes.....	6
2.2	General.....	6
2.2.1	NokiaIPSecVPN.....	6
2.2.2	NokiaIPSecVPN/General .....	7
2.2.3	NokiaIPSecVPN/General/ClientVersion.....	7
2.2.4	NokiaIPSecVPN/General/EventLog.....	7
2.3	VPN access points.....	7
2.3.1	NokiaIPSecVPN/AP .....	8
2.3.2	NokiaIPSecVPN/AP/<X> .....	8
2.3.3	NokiaIPSecVPN/AP/<X>/Name.....	9
2.3.4	NokiaIPSecVPN/AP/<X>/ThisRef.....	9
2.3.5	NokiaIPSecVPN/AP/<X>/PolicyRef.....	9
2.3.6	NokiaIPSecVPN/AP/<X>/PolicyRef/ID.....	10
2.3.7	NokiaIPSecVPN/AP/<X>/PolicyRef/URI .....	10
2.3.8	NokiaIPSecVPN/AP/<X>/ConRef.....	10
2.4	VPN policies.....	11
2.4.1	NokiaIPSecVPN/Policy.....	11
2.4.2	NokiaIPSecVPN/Policy/<X>/ .....	11
2.4.3	NokiaIPSecVPN/Policy/<X>/Name .....	11
2.4.4	NokiaIPSecVPN/Policy/<X>/ID.....	11
2.4.5	NokiaIPSecVPN/Policy/<X>/Version .....	12
2.4.6	NokiaIPSecVPN/Policy/<X>/Description.....	12
2.4.7	NokiaIPSecVPN/Policy/<X>/Issuer .....	12
2.4.8	NokiaIPSecVPN/Policy/<X>/Contact .....	13
2.4.9	NokiaIPSecVPN/Policy/<X>/Content.....	13
<b>3</b>	<b>Management object usage</b> .....	<b>14</b>
3.1	General.....	14
3.2	VPN access point management (AP node).....	14
3.3	VPN policy management (Policy node).....	15
<b>4</b>	<b>Terms and abbreviations</b> .....	<b>17</b>
<b>5</b>	<b>References</b> .....	<b>18</b>
<b>6</b>	<b>Evaluate this resource</b> .....	<b>19</b>

## Change history

April 30, 2007	Version 1.0	Initial document release

# 1 Introduction

This document describes an OMA Device Management (DM) (for more information, see reference document [1]) management object for the configuration of the Nokia Mobile VPN Client software (for more information, see reference document [2]). This document is applicable for S60 3rd Edition, Feature Pack 1 devices.

## 1.1 Supported management operations

Management servers can use the VPN client management object to list, get, add, update, and delete VPN access points and VPN policies. PKI-related management operations that are needed to set up a complete working VPN configuration to clients are performed through the PKI management object described in reference document [9].

The setup of other applications, such as e-mail, to refer to VPN access points in their configuration must be done through the general AP management node (for more information, see reference document [4]).

## 1.2 Supported manageable data

The VPN client management object allows management servers to manage both data that has been initially added to devices via OMA DM and data that has been added to devices through some other mechanisms (for example through the UI of the device).

## 1.3 Documentation conventions

Device management command examples are written with the `Courier` font.

The dynamic name of a management node is denoted with `<X>`. The name must be unique among its siblings. For OMA DM server-added VPN management objects, the OMA DM server selects the names for the nodes according to server-specific rules. The VPN client automatically creates the names for the nodes that are configured to the system through non OMA DM mechanisms. For such nodes, the name of the node is a random number formatted as a string and prefixed with the string "cli", for example "cli123".

## 2 VPN management object nodes

This chapter describes the management nodes that constitute the VPN client management object. The Device Description Framework properties (Scope, Occurrence, Access type, Format, and Value) used in the descriptions are defined in reference document [5].

All URI values in the management object are given with the root of the management tree as the starting point. As specified in reference document [5], this can be denoted by beginning each URI with “./” or “” (nothing).

### 2.1 List of management nodes

The list below summarizes all management nodes described later in this document.

- NokiaIPSecVPN (see Section 2.2.1)
- NokiaIPSecVPN/General (see Section 2.2.2)
- NokiaIPSecVPN/General/ClientVersion (see Section 2.2.3)
- NokiaIPSecVPN/General/EventLog (see Section 2.2.4)
- NokiaIPSecVPN/AP (see Section 2.3.1)
- NokiaIPSecVPN/AP/<X> (see Section 2.3.2)
- NokiaIPSecVPN/AP/<X>/Name (see Section 2.3.3)
- NokiaIPSecVPN/AP/<X>/ThisRef (see Section 2.3.4)
- NokiaIPSecVPN/AP/<X>/PolicyRef (see Section 2.3.5)
- NokiaIPSecVPN/AP/<X>/PolicyRef/ID (see Section 2.3.6)
- NokiaIPSecVPN/AP/<X>/PolicyRef/URI (see Section 2.3.7)
- NokiaIPSecVPN/AP/<X>/ConRef (see Section 2.3.8)
- NokiaIPSecVPN/Policy (see Section 2.4.1)
- NokiaIPSecVPN/Policy/<X>/ (see Section 2.4.2)
- NokiaIPSecVPN/Policy/<X>/Name (see Section 2.4.3)
- NokiaIPSecVPN/Policy/<X>/ID (see Section 2.4.4)
- NokiaIPSecVPN/Policy/<X>/Version (see Section 2.4.5)
- NokiaIPSecVPN/Policy/<X>/Description (see Section 2.4.6)
- NokiaIPSecVPN/Policy/<X>/Issuer (see Section 2.4.7)
- NokiaIPSecVPN/Policy/<X>/Contact (see Section 2.4.8)
- NokiaIPSecVPN/Policy/<X>/Content (see Section 2.4.9)

### 2.2 General

#### 2.2.1 NokiaIPSecVPN

The NokiaIPSecVPN interior node is the parent of VPN client management tree nodes. If this node can be found from a client’s management tree, then the client can be assumed to support all management nodes under this parent node.

The name and version of the VPN client management object described in this document is 'com.nokia.devman/1.0/ipsecvpn'. It is defined in the Type property of the NokiaIPSecVPN node.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

### 2.2.2 NokiaIPSecVPN/General

This interior node is the parent of management nodes that describe general information about the VPN client software and the management object.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

### 2.2.3 NokiaIPSecVPN/General/ClientVersion

This leaf node specifies the version of the Nokia Mobile VPN Client software present in the device.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	The version of the Nokia Mobile VPN Client software that is in the device. For example, "3_1_070809".	

### 2.2.4 NokiaIPSecVPN/General/EventLog

This leaf node represents the event log maintained by the VPN client software. A `Get` command on the node can be used to fetch the event log data from the client and a `Delete` command on the node can be used to clear the event log.

Scope	Occurrence	Access type
Dynamic	One	Get, Delete
Format	Value	
Chr	The contents of the event log.	

## 2.3 VPN access points

This section describes the management tree structure and management nodes that can be used to manage VPN access points.

Management operations that require references to VPN access points require the use of the general AP node (for more information, see reference document [4]). This is because other management objects and the respective management adapters are only aware about the general AP node. The general AP

node cannot be used for all VPN access point management operations, because it lacks knowledge about the VPN-specific configuration parameters and their handling.

Table 1 lists the different management operations and the management tree branch that can be used in each operation.

Management operation	NokiaIPSecVPN/AP	AP
List VPN access points	Yes	Yes
Get information about a single VPN access point	Yes*	Yes*
Add a VPN access point	Yes*	No*
Update a VPN access point	Yes*	No*
Delete a VPN access point	Yes*	No*

Table 1: The management operations and management tree branch that can be used in each operation

\* The proxy information related to VPN access points is always managed through the general AP node.

Some important points to note:

- Only VPN access points appear under the NokiaIPSecVPN/AP node.
- All access points appear under the general AP node, including VPN access points.
- When listing access points through the general AP node, VPN access points may be differentiated from the other access points based on the bearer network type (./AP/<x>/NAPDef/<x>/Bearer/<x>/BearerL="VPN").
- The name of a certain VPN access point is the same in both the NokiaIPSecVPN/AP and general AP tree branches.
- The URIs of management nodes representing the same VPN access point in the NokiaIPSecVPN/AP and general AP tree branches have a different dynamic part (<X>).

The management nodes that constitute the VPN access point management object are described below.

### 2.3.1 NokiaIPSecVPN/AP

This interior node is the parent of all management tree nodes that are used to manage VPN access points.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

### 2.3.2 NokiaIPSecVPN/AP/<X>

This interior node together with its descendant nodes represents a single VPN access point. An access point should be added to and deleted from a client as a single entity. To delete an access point from a device, the management server should issue a single `Delete` command on a VPN access point node (<X>).

A VPN access point added to a client through this node becomes visible also in the general AP tree branch. The node representing a VPN access point in the general AP branch is the node that must be

used when the VPN access point needs to be referred to from some other parts of the management tree.

Scope	Occurrence	Access type
Dynamic	ZeroOrMore	Add, Delete, Get
Format	Value	
Node		

### 2.3.3 NokiaIPSecVPN/AP/<X>/Name

This leaf node contains a human-readable name of the VPN access point.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	A sequence of 1 to 50 Unicode characters. Leading and trailing white space, tabs, new lines, and other control characters are not allowed in the name. When adding or replacing the name, if the value contains illegal characters or is otherwise incorrectly formatted, the client returns status code 412 (incomplete command).	

### 2.3.4 NokiaIPSecVPN/AP/<X>/ThisRef

This leaf node specifies the URI of the management node that represents this VPN access point in the general AP tree branch. This is the URI that can be used to refer to the VPN access point from other parts of the management tree. Note that this node is read-only.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	The URI of the management node that represents the VPN access point in the general AP tree branch. The URI is given relative to the management tree root and does not use the “./” prefix. For example: “AP/APId003”.	

### 2.3.5 NokiaIPSecVPN/AP/<X>/PolicyRef

This interior node is the parent of management nodes that are used to manage the association of a VPN access point with a VPN policy.

Scope	Occurrence	Access type
Dynamic	One	Add, Get
Format	Value	
Node		

### 2.3.6 NokiaIPSecVPN/AP/<X>/PolicyRef/ID

This leaf node specifies the globally unique ID of the VPN policy that is associated with the access point. The setting and changing of a VPN access point's policy association is handled through this node. The use of an ID instead of a management tree URI for the association brings more flexibility to the association handling. For example, a VPN access point can be added to a client before or after the associated policy.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	The globally unique ID of the associated VPN policy. The value of this field can also be empty, in which case the access point is not associated with any policy. The value is the same as the value of some NokiaIPSecVPN/Policy/<X>/ID node, for example "456".	

### 2.3.7 NokiaIPSecVPN/AP/<X>/PolicyRef/URI

This leaf node specifies the management tree URI of the VPN policy that is associated with the VPN access point. Note that this node is read-only as the actual management of a VPN access point's policy association is handled through the ID node described in Section 2.3.6. This node can be useful in situations where the management server has read an access point definition from a client and then wants to directly access the associated VPN policy.

Scope	Occurrence	Access type
Dynamic	One	Get
Format	Value	
Chr	The URI of the associated VPN policy node in the management tree. The value can be empty if the associated policy is not present in the client. The URI is given relative to the management tree root and does not use the "." prefix. For example "NokiaIPSecVPN/Policy/123".	

### 2.3.8 NokiaIPSecVPN/AP/<X>/ConRef

This leaf node specifies the association of the VPN access point with the real access point through which the VPN client software communicates with the VPN gateway.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	The management tree URI of the associated access point. In the Add and Replace commands, the value cannot be empty. In the Get command, the returned value can be empty, if the associated access point or network is not present in the client. The URI is given relative to the management tree root and does not use the "." prefix. For example, "AP/123".	

## 2.4 VPN policies

This section describes the management tree structure and management nodes that can be used to manage VPN policies.

### 2.4.1 NokiaIPSecVPN/Policy

This interior node is the parent of all management tree nodes that are used to manage VPN policies.

Scope	Occurrence	Access type
Permanent	One	Get
Format	Value	
Node		

### 2.4.2 NokiaIPSecVPN/Policy/<X>/

This interior node, together with its descendant nodes, represents a single VPN policy. A VPN policy should be added to and deleted from a client as a single entity. To delete a VPN policy from a device, the management server should issue a single `Delete` command on a policy node (<X>).

Scope	Occurrence	Access type
Dynamic	ZeroOrMore	Add, Delete, Get
Format	Value	
Node		

### 2.4.3 NokiaIPSecVPN/Policy/<X>/Name

This leaf node specifies the name of the VPN policy.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	A sequence of 1 to 128 Unicode characters. Leading and trailing white space, tabs, newlines and other control characters are not allowed in the name. When adding or replacing the name, if the value contains illegal characters or is otherwise incorrectly formatted, the client returns status code 412 (incomplete command).	

### 2.4.4 NokiaIPSecVPN/Policy/<X>/ID

This leaf node specifies a unique ID of the policy. This ID identifies the policy uniquely even across different devices and also outside the OMA DM domain. It is up to the management servers to define the ID in a way that fulfills the uniqueness requirement. Only a single policy can have the same ID value in the client.

Scope	Occurrence	Access type
Dynamic	One	Add, Get
Format	Value	
Chr	<p>A sequence of 1 to 50 Unicode characters. Leading and trailing white space, tabs, newlines and other control characters are not allowed in the ID. When adding or replacing the ID, if the value contains illegal characters or is otherwise incorrectly formatted, the client returns status code 412 (incomplete command).</p> <p>For example a string representation of a Universally Unique ID (UUID) as defined in reference document [4]: "f81d4fae-7dec-11d0-a765-00a0c91e6bf6".</p>	

#### 2.4.5 NokiaIPSecVPN/Policy/<X>/Version

This leaf node specifies the version of the policy. Note that this is different from the policy format version that is specified inside the policy content.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	<p>A sequence of 0 to 16 Unicode characters. The format of the version value is &lt;major-version&gt;'.&lt;minor-version&gt;, where major-version and minor-version are strings representing positive integers. For example "1.0".</p>	

#### 2.4.6 NokiaIPSecVPN/Policy/<X>/Description

This leaf node contains a description of the policy.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	A sequence of 0 to 256 Unicode characters.	

#### 2.4.7 NokiaIPSecVPN/Policy/<X>/Issuer

This leaf node identifies the issuer of the VPN policy.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	A sequence of 0 to 128 Unicode characters.	

## 2.4.8 NokiaIPSecVPN/Policy/&lt;X&gt;/Contact

This leaf node specifies contact information for the policy.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	A sequence of 0 to 128 Unicode characters. For example a phone number, e-mail address, or URL.	

## 2.4.9 NokiaIPSecVPN/Policy/&lt;X&gt;/Content

This leaf node stores the actual VPN policy content as a single large text object.

Scope	Occurrence	Access type
Dynamic	One	Add, Get, Replace
Format	Value	
Chr	<p>The policy content in the format described in reference document [2].</p> <p>In the OMA DM case VPN policies must not refer to CA certificates via file names (<code>FORMAT: BIN</code>). Instead, the references are be expressed in the form of CA subject names (<code>FORMAT: NAME</code>), application UIDs (<code>FORMAT: APPLUID</code>), or key identifier (<code>FORMAT: KEYID</code>).</p> <p>The <code>FORMAT</code>, <code>DATA</code>, <code>PRIVATE_KEY_FORMAT</code> and <code>PRIVATE_KEY_DATA</code> fields in the <code>OWN_CERTS</code> section are not applicable to the OMA DM case.</p>	

### 3 Management object usage

This chapter describes how management servers should use the VPN client management object to perform management operations.

#### 3.1 General

Management operation	Implementation
Find out the version of the VPN client management object that the client supports	Get command on the NokiaIPSecVPN node's Type property. GET ./NokiaIPSecVPN?prop=Type
Find out the version of the VPN client software	Get command on the NokiaIPSecVPN/General/ClientVersion node. GET ./NokiaIPSecVPN/General/ClientVersion
Fetch the VPN client event log from the client	Get command on the NokiaIPSecVPN/General/EventLog node. GET ./NokiaIPSecVPN/General/EventLog
Clear the VPN client event log at the client	Delete command on the NokiaIPSecVPN/General/EventLog node. DELETE ./NokiaIPSecVPN/General/EventLog

#### 3.2 VPN access point management (AP node)

Management operation	Implementation
List VPN access points	Multiple Get commands under the NokiaIPSecVPN/AP or general AP node in multiple OMA DM request messages.  For example: // First OMA DM request message: GET ./NokiaIPSecVPN/AP  // Second OMA DM request message // (100, 101 and 102 are dynamic // node names returned by the first // OMA DM request message: GET ./NokiaIPSecVPN/AP/100/Name GET ./NokiaIPSecVPN/AP/101/Name GET ./NokiaIPSecVPN/AP/102/Name ...
Add VPN access point	Add commands within the AP node. For example: ADD ./NokiaIPSecVPN/AP/103="" ADD ./NokiaIPSecVPN/AP/103/Name="VPN AP"  ADD ./NokiaIPSecVPN/AP/103/PolicyRef="" ADD ./NokiaIPSecVPN/AP/103/PolicyRef/ID="123" ADD ./NokiaIPSecVPN/AP/103/ConRef="AP/AP01"

Update VPN access point	Replace command on an access point node. For example REPLACE ./NokiaIPSecVPN/AP/103/Name="VPN"
Delete VPN access point	Delete command on an access point node. For example DELETE ./NokiaIPSecVPN/AP/103
Set VPN access point proxy information	Add commands within the general AP node (see reference document [4]). In the example below, APid001 is a dynamic node name of the access point. ADD ./AP/APid001/Px="" ADD ./AP/APid001/Px/1="" ADD ./AP/APid001/Px/1/PxAddr="example.com" ADD ./AP/APid001/Px/1/Startpg="www.example.com" ADD ./AP/APid001/Px/1/Port/PROXY="" ADD ./AP/APid001/Px/1/Port/PROXY/PortNbr="80"

### 3.3 VPN policy management (Policy node)

Management operation	Implementation
List VPN policies	Policy listing is done by issuing multiple Get commands under the NokiaIPSecVPN/Policy node in multiple OMA DM request messages. For example: // First OMA DM request message: GET ./NokiaIPSecVPN/Policy  // Second OMA DM request message // (100and 101 are dynamic // node names returned by the first // OMA DM request message: GET ./NokiaIPSecVPN/Policy/100/Name GET ./NokiaIPSecVPN/Policy/100/ID GET ./NokiaIPSecVPN/Policy/101/Name GET ./NokiaIPSecVPN/Policy/101/ID ...
Add VPN policy	Add commands within the Policy node. For example: ADD ./NokiaIPSecVPN/Policy/102="" ADD ./NokiaIPSecVPN/Policy/102/Name="name" ADD ./NokiaIPSecVPN/Policy/102/ID="123" ADD ./NokiaIPSecVPN/Policy/102/Version="1.0" ADD ./NokiaIPSecVPN/Policy/102/Description="desc" ADD ./NokiaIPSecVPN/Policy/102/Issuer="issuer" ADD ./NokiaIPSecVPN/Policy/102/Contact="contact" ADD ./NokiaIPSecVPN/Policy/102/Content="<data>" In the example above, <data> denotes policy content in the format described in reference document [2].

Update VPN policy	Replace commands on a policy node. For example: REPLACE ./NokiaIPSecVPN/Policy/102/Version="1.1"
Delete VPN policy	Delete command on a policy node. For example: DELETE ./NokiaIPSecVPN/Policy/102
Get actual VPN policy content	Get command on a policy content node. For example: GET ./NokiaIPSecVPN/Policy/102/Content

## 4 Terms and abbreviations

Term or abbreviation	Meaning
ACL	Access Control List
AP	Access Point
CA	Certificate Authority
Client	A mobile device running the Nokia Mobile VPN Client software with OMA DM client support.
DDF	Device Description File
DM	Device Management
General AP node, general AP tree	These terms refer to the ./AP node defined in the Connectivity Settings management object (see reference document [9]).
IP	Internet Protocol
IPsec	IP Security Protocol
Management server	An OMA DM server.
OMA	Open Mobile Alliance
PKI	Public Key Infrastructure
PKI store	A client-side centralized storage for PKI objects.
URI	Uniform Resource Identifier
User certificate	A user is authenticated with a user certificate. If a user certificate is stored to device store, it means that in practice only the device is authenticated.
VPN	Virtual Private Network
XML	Extensible Markup Language

## 5 References

- [1] Enabler Release Definition for OMA Device Management (based on SyncML DM), OMA-ERELED-SyncML\_DM-V1\_1\_2-20031209-A.pdf, available at <http://www.openmobilealliance.org/>
- [2] Mobile VPN Client Policy File Format
- [3] Nokia Mobile VPN, available at <http://www.nokia.com>
- [4] [OMA DM: Management Object for Connectivity Settings](http://www.forum.nokia.com/), available at <http://www.forum.nokia.com/>
- [5] SyncML Device Management Tree and Description, Version 1.1.2 (OMA-SyncML-DMTND-V1\_1\_2-20031202-A.pdf), available at <http://www.openmobilealliance.org/>
- [6] SyncML Representation Protocol Device Management Usage (OMA-SyncML-DMRepPro-V1\_1\_2-20030613-A.doc) , available at <http://www.openmobilealliance.org/>
- [7] SyncML Representation Protocol (OMA-SyncML-RepPro-V1\_1\_2-20040711-A.doc) , available at <http://www.openmobilealliance.org/>
- [8] A Universally Unique Identifier (UUID) URN Namespace (RFC 4122) , available at <http://www.ietf.org>
- [9] [VPN Client PKI Management Object Specification](http://www.forum.nokia.com), available at <http://www.forum.nokia.com>

## 6 Evaluate this resource

Please spare a moment to help us improve documentation quality and recognize the resources you find most valuable, by [rating this resource](#).